User's Guide

TRENDnet®

N300 Wireless Router

TEW-732BR

Contents

Product Overview 3

Package Contents 3

Features 3

Product Hardware Features 4

Application Diagram 5

Basic Router Setup 6

Creating a Home Network 6

Router Installation 7

Connect additional wired devices to your network 10

Wireless Networking and Security 10

How to choose the type of security for your wireless network 10

Secure your wireless network 11

Connect wireless devices to your router 13

Connect wireless devices using WPS 14

Basic wireless settings 15

Steps to improve wireless connectivity 16

Advanced wireless settings 17

Access Control Filters 17

Access control basics 17

MAC address filters 17

Domain/URL Filters 18

Protocol/IP filters 19

Advanced Router Setup 21

Access your router management page 21

Change your router login password 21

Set your router date and time 22

Manually configure your Internet connection 22

Clone a MAC address 23

Change your router IP address 23

Set up the DHCP server on your router 24

Set up DHCP reservation 25

Enable/disable UPnP on your router 25

Allow/deny VPN connections through your router 26

Allow/deny multicast streaming 26

Identify your network on the Internet 26

Allow remote access to your router management page 27

Open a device on your network to the Internet 27

DMZ 27

Virtual Server 28

Special Applications 29

Add static routes to your router 31

Router Maintenance & Monitoring 31

Reset your router to factory defaults 31

Router Default Settings 32

Backup and restore your router configuration settings 32

Upgrade your router firmware 33

Restart your router 34

Check connectivity using the router management page 34

Check the router system information 34

View your router log 35

Configure your router log 36

© Copyright 2012 TRENDnet. All Rights Reserved.

View your router packet statistics 37

View wireless devices connected to your router..... 38

Router Management Page Structure 39

Technical Specifications.....40

Troubleshooting.....41

Appendix 42

© Copyright 2012 TRENDnet. All Rights Reserved.

Product Overview

TEW-732BR

Package Contents

In addition to your router, the package includes:

- Multi-Language Quick Installation Guide
- CD-ROM (User's Guide)
- Network cable (1.5 m / 5 ft.)
- Power adapter (5V DC, 1A)

If any package contents are missing or damaged, please contact the retail store, online retailer, or reseller/distributor from which the product was purchased.

Features

TRENDnet's N300 Wireless Router, model TEW-732BR, offers proven 300 Mbps wireless n networking to share files, play games, and surf the internet. Embedded GREENnet technology reduces power consumption by up to 50%. For your security this router comes pre-encrypted. OpenSource compatible firmware facilitates user-based customization.

Ease of Use

Easy Setup
Get up and running in minutes with the intuitive guided setup
One Touch Connection
Securely connect to the router at the touch of the Wi-Fi Protected Setup (WPS) button

Security

Pre-Encrypted
For your security the router is pre-encrypted with a unique password
Parental Controls
Control access to specific websites

Performance

N300 Wireless
Proven 300 Mbps Wireless N
Ethernet Ports
Ethernet ports to hardwire up to four devices
Wireless Coverage
Whole home wireless coverage with MIMO antenna technology for average size homes
OpenSource
OpenSource compatible firmware facilitates user-based customization
Quality of Service (QoS)
Advanced QoS prioritizes video and audio transmissions

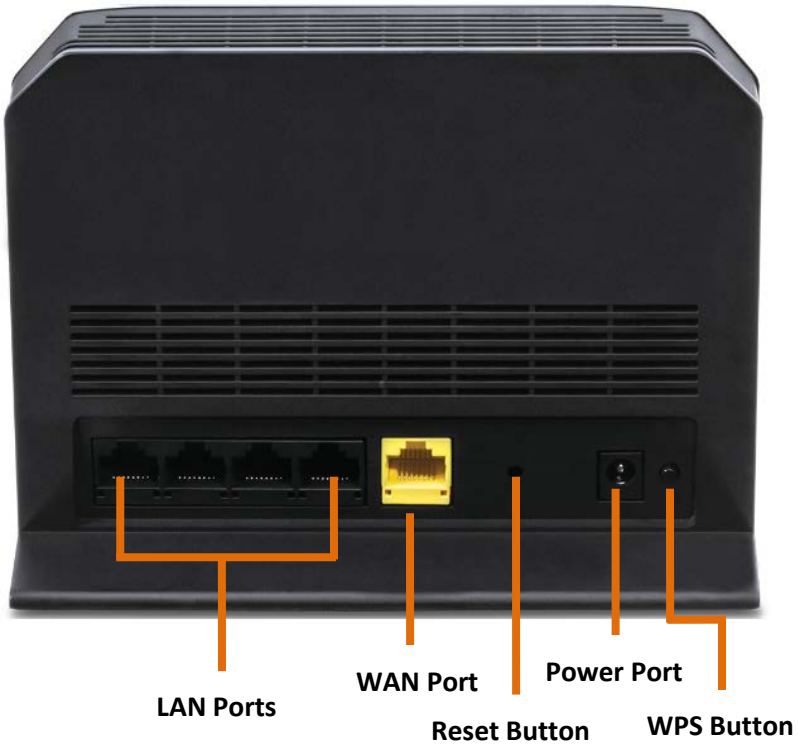
© Copyright 2013 TRENDnet. All Rights Reserved.

Compatibility
Compatible with older Wireless G devices
Energy Savings
Embedded GREENnet technology reduces power consumption by up to 50%
IPv6
IPv6 network support

*Maximum wireless signal rates are referenced from IEEE 802.11 theoretical specifications. Actual data throughput and coverage will vary depending on interference, network traffic, building materials and other conditions.

Product Hardware Features

Rear View



- **LAN Ports:** Connect Ethernet cables (also called network cables) from your router LAN ports to your wired network devices.
- **WAN Port:** Connect an Ethernet cable from your router WAN port to your modem.
- **Reset Button:** Use an item such as a paperclip to push and hold this button for 5 seconds and release to reset your router to its factory defaults.
- **Power Port:** Connect the included power adapter from your router power port and to an available power outlet.

© Copyright 2013 TRENDnet. All Rights Reserved.

- **WPS (Wi-Fi Protected Setup):** Push and hold this button for 3 seconds to activate WPS. The button LED is blinking blue when WPS is activated.
- **On/Off Power Switch (EU only):** Push the router On/Off power switch to turn your router "On" (Inner position) or "Off" (Outer position).

Front View

- **Power LED:** This LED indicator is solid green when your router is powered on. Otherwise if this LED indicator is off, there is no power to your router.
- **WAN (Link/Activity) LED:** This LED indicator is solid green when your router WAN port is physically connected to the modem Network port (also called network port) successfully with a Network cable. The LED indicator will be blinking green while data is transmitted or received through the WAN port of your router.

Application Diagram

The router is installed near the modem (typically supplied by your ISP "Internet Service Provider") and physically connected to it from the router's Internet port to the modem's network port which connects to the Internet. 2.4GHz wireless signals from the router are broadcasted to wireless clients such as laptops (with wireless capability).

© Copyright 2013 TRENDnet. All Rights Reserved.

Basic Router Setup

Creating a Home Network

What is a network?

A network is a group of computers or devices that can communicate with each other. A home network of more than one computer or device also typically includes Internet access, which requires a router.

A typical home network may include multiple computers, a media player/server, a printer, a modem, and a router. A large home network may also have a switch, additional routers, access points, and many Internet-capable media devices such as TVs, game consoles, and Internet cameras.

- **Modem:** Connects a computer or router to the Internet or ISP (Internet Service Provider).
- **Router:** Connects multiple devices to the Internet.
- **Switch"**Connect several wired network devices to your home network. Your router has a built-in network switch (the LAN port 1-4). If you have more wired network devices than available Ethernet ports on your router, you will need an additional switch to add more wired connections.

How to set up a home network

1. For a network that includes Internet access, you'll need:
   - **Computers/devices with an Ethernet port (also called network port) or wireless networking capabilities.**
   - **A modem and Internet service to your home, provided by your ISP (modem typically supplied by your ISP).**
   - **A router to connect multiple devices to the Internet.**
2. Make sure that your modem is working properly. Your modem is often provided by your Internet Service Provider (ISP) when you sign up for Internet service. If your modem is not working contact your ISP to verify functionality.
3. Set up your router. See "How to setup your router" below.
4. To connect additional wired computers or wired network devices to your network, see "Connect additional wired devices to your network" on page 10.
5. To set up wireless networking on your router, see "Secure your wireless network" on page 11.

How to setup your router

Refer to the Quick Installation Guide or continue to the next section "Router Installation" on page 7 for more detailed installation instructions.

Where to find more help

In addition to this User's Guide, you can find help below:

- http://www.trendnet.com/support
  (documents, downloads, and FAQs are available from this Web page)

© Copyright 2013 TRENDnet. All Rights Reserved.

Router Installation

Before you Install

Many Internet Service Providers (ISPs) allow your router to connect to the Internet without verifying the information fields listed below. Skip this section for now and if your router cannot connect to the Internet using the standard installation process, come back to this page and contact your ISP to verify required ISP specification fields listed below.

1. Obtain IP Address Automatically (DHCP)
Host Name (Optional)
Clone Mac Address (Optional)

2. Fixed IP address
WAN IP Address: _____. _____._____._____
(e.g. 215.24.24.129)
WAN Subnet Mask: _____. _____._____._____
WAN Gateway IP Address: _____. _____._____._____
DNS Server Address 1: _____. _____._____._____
DNS Server Address 2: _____. _____._____._____

3. PPPoE to obtain IP automatically
User Name: _____
Password: _____
Verify Password: _____

4. PPPoE with a fixed IP address
User Name: _____
Password: _____
Verify Password: _____
IP Address: ____. _____._____._____ (e.g. 215.24.24.129)

5. PPTP or Russian PPTP
Type (Dynamic IP or Static IP)
My IP Address: _____. _____._____._____
(e.g. 215.24.24.129)
Subnet Mask:_____. _____._____._____
Gateway:_____. _____._____._____
Server IP: _____. _____._____._____
PPTP Account: _____
PPTP Password: _____
Retype Password: _____

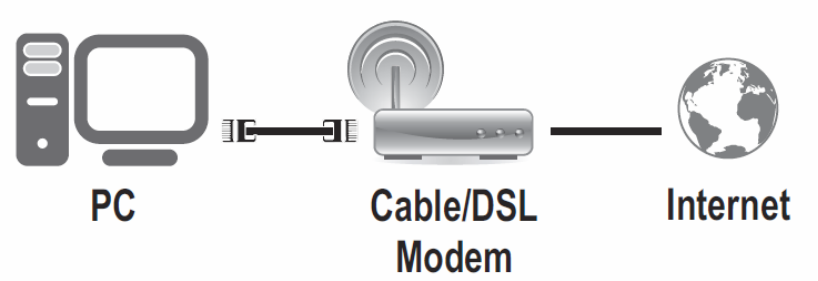
6. L2TP or Russia L2TP
Type (Dynamic IP or Static IP)
My IP Address: _____. _____._____._____
(e.g. 215.24.24.129)
Subnet Mask:_____. _____._____._____
Gateway:_____. _____._____._____
Server IP: _____. _____._____._____
L2TP Account: _____
L2TP Password: _____
Retype Password: _____

7. Russia PPPoE
Type (Dynamic IP or Static IP)
User Name: _____
Password: _____
Verify Password: _____
IP Address: ____. _____._____._____ (e.g. 215.24.24.129)

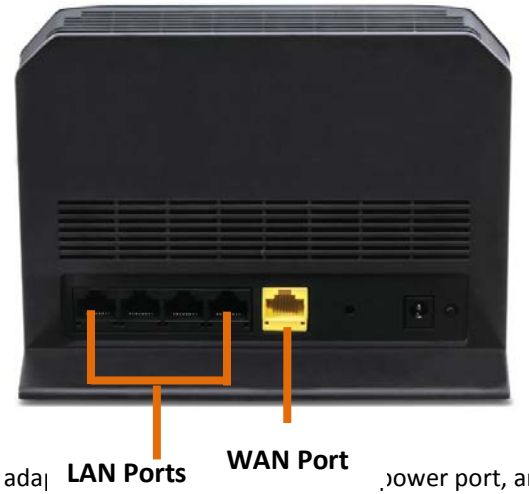
© Copyright 2013 TRENDnet. All Rights Reserved.

Hardware Installation

1. Verify that you have an Internet connection when connecting your computer directly to your modem.



2. Turn off your modem.
3. Disconnect the Network cable from your computer to your modem.
4. Using a Network cable, connect the WAN port on the router to your modem.
5. Using another Network cable, connect your computer to one of the four LAN ports on the router.



6. Plug in the power ada| .)ower port, and then push the On/Off Power Switch to the "On" position (pushed in).

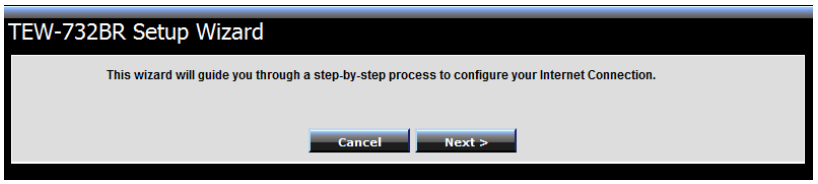
Power Port

7. Turn on your modem.
8. Verify that the following front panel LED indicators on your router: Power (Solid Green), WAN (Solid/Blinking Green).

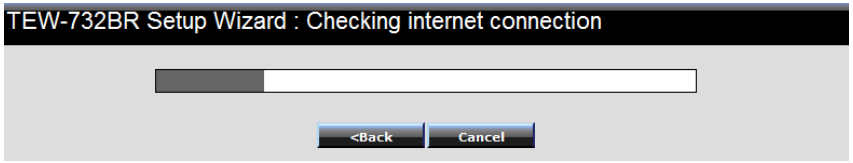
© Copyright 2013 TRENDnet. All Rights Reserved.

Setup Wizard

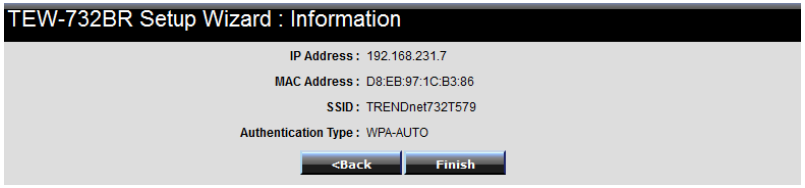
1. Open your web browser (e.g. Internet Explorer, Firefox, Safari, Chrome, or Opera) and the installation wizard will automatically appear. Click **Next** to continue.


TEW-732BR Setup Wizard
This wizard will guide you through a step-by-step process to configure your Internet Connection.
Cancel
Next >

2. Your router will scan for Internet connection and type.



3. Once the router detects Internet connection your installation is complete. Verify your settings and click Finish to complete installation.



4. Open a new tab on your web browser and enter in a website (e.g. www.trendnet.com) to verify that you have an Internet connection.

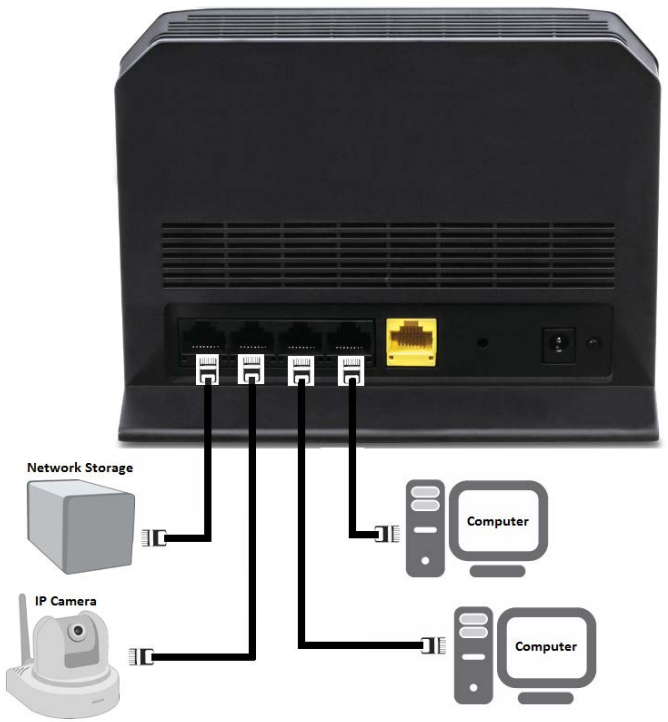
5. For added security, the router is pre-encrypted with its own unique wireless network security key. You can find the unique network security key and pre-assigned network name (SSID) on a sticker on the front of the router and on a label on the back of the router. If you would like to change the wireless security settings refer to "Secure your wireless network" section on page 11.

© Copyright 2013 TRENDnet. All Rights Reserved.

Connect additional wired devices to your network

You can connect additional computers or other network enabled devices to your network by using Ethernet cables to connect them to one of the available LAN ports labeled 1,2,3,4 on your router. Check the status of the LED indicators (1, 2, 3, or 4) on the front panel of your router to ensure the physical cable connection from your computer or device.

Note: *If you encounter issues connecting to your network, there may be a problem with your computer or device network settings. Please ensure that your computer or device network settings (also called TCP/IP settings) are configured to obtain IP address settings automatically (also called dynamic IP address or DHCP) and to Obtain DNS Server address settings automatically.*



Wireless Networking and Security

How to choose the type of security for your wireless network

Setting up wireless security is very important. Leaving your wireless network open and unsecure could expose your entire network and personal files to outsiders. TRENDnet recommends reading through this entire section and setting up wireless security on your new router.

There are a few different wireless security types supported in wireless networking each having its own characteristics which may be more suitable for your wireless network taking into consideration compatibility, performance, as well as the security strength along with using older wireless networking hardware (also called legacy hardware).
It is strongly recommended to enable wireless security to prevent unwanted users from accessing your network and network resources (personal documents, media, etc.).
In general, it is recommended that you choose the security type with the highest strength and performance supported by the wireless computers and devices in your network. Please review the security types to determine which one you should use for your network.

Wireless Encryption Types

- **WEP:** Legacy encryption method supported by older 802.11b/g hardware. This is the oldest and least secure type of wireless encryption. It is generally not recommended to use this encryption standard, however if you have old 802.11 b or 802.11g wireless adapters or computers with old embedded wireless cards(wireless clients), you may have to set your router to WEP to allow the old adapters to connect to the router. ***Note****: This encryption standard will limit connection speeds to 54Mbps.*
- **WPA:** This encryption is significantly more robust than the WEP technology. Much of the older 802.11g hardware was been upgraded (with firmware/driver upgrades) to support this encryption standard. Total wireless speeds under this encryption type however are limited to 54Mbps.
- **WPA-**Auto: This setting provides the router with the ability to detect wireless devices using either WPA or WPA2 encryption. Your wireless network will automatically change the encryption setting based on the first wireless device connected. For example, if the first wireless client that connects to your wireless

© Copyright 2013 TRENDnet. All Rights Reserved.

network uses WPA encryption your wireless network will use WPA encryption. Only when all wireless clients disconnect to the network and a wireless client with WPA2 encryption connects your wireless network will then change to WPA2 encryption. NOTE: WPA2 encryption supports 802.11n speeds and WPA encryption will limit your connection speeds to 54Mbps

- **WPA2:** This is the most secure wireless encryption available today, similar to WPA encryption but more robust. This encryption standard also supports the highest connection speeds. TRENDnet recommends setting your router to this encryption standard. If you find that one of your wireless network devices does not support WPA2 encryption, then set your router to either WPA or WPA-Auto encryption.
  Note: *Check the specifications of your wireless network adapters and wireless appliances to verify the highest level of encryption supported.*
  Below is brief comparison chart of the wireless security types and the recommended configuration depending on which type you choose for your wireless network.

Security Standard	WEP	WPA	WPA2
Compatible Wireless Standards	IEEE 802.11a/b/g (802.11n devices will operate at 802.11g to connect using this standard)	IEEE 802.11a/b/g (802.11n devices will operate at 802.11g to connect using this standard)	IEEE 802.11a/b/g/n
Highest Performance Under This Setting	**Up to 54Mbps**	**Up to 54Mbps**	**Up to 3000Mbps***
Encryption Strength	Low	Medium	High
Additional Options	Open System or Shared Key, HEX or ASCII, Different key sizes	TKIP or AES, Preshared Key or RADIUS	TKIP or AES, Preshared Key or RADIUS
Recommended Configuration	Open System ASCII 13 characters	TKIP Preshared Key 8-63 characters	AES Preshared Key 8-63 characters

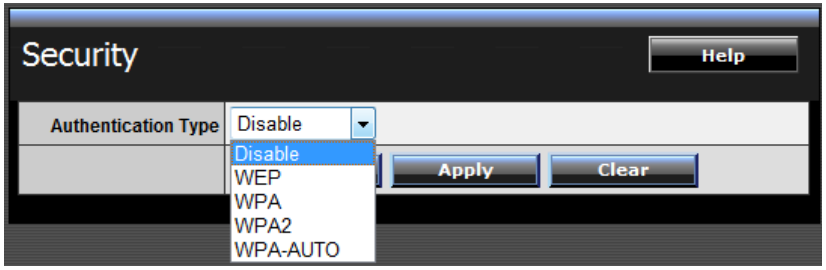
*Dependent on the maximum 802.11n data rate supported by the device (150Mbps, or 300Mbps)

Secure your wireless network

Wireless > Security

After you have determined which security type to use for your wireless network (see "How to choose the security type for your wireless network" on page 11), you can set up wireless security.

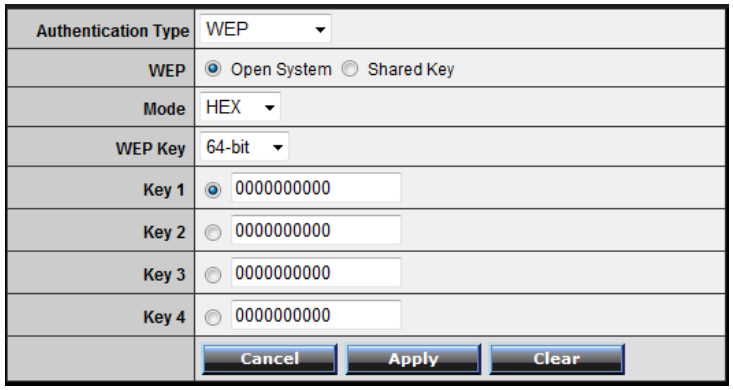
1. Log into your router management page (see "Access your router management page" on page 21).
2. Click on **Wireless**, and click on **Security**.
3. Click on the **Authentication Type** drop-down list to select your wireless security type.



© Copyright 2013 TRENDnet. All Rights Reserved.

Selecting WEP:

If selecting **WEP** (Wired Equivalent Privacy), please review the WEP settings to configure and click **Apply** to save the changes.



- **WEP**– Choose **Open System** or **Shared Key**.
  Note: *It is recommended to use Open System because it is known to be more secure than Shared Key.*
- **Mode** – Choose **HEX** or **ASCII**.
  Note: *It is recommended to use ASCII because of the much larger character set that can be used to create the key.*
- **WEP Key** – Choose the key length **64-bit** or **128-bit**.
  Note: *It is recommended to use 128-bit because it is more secure to use a key that consists of more characters.*

- **Key 1-4**

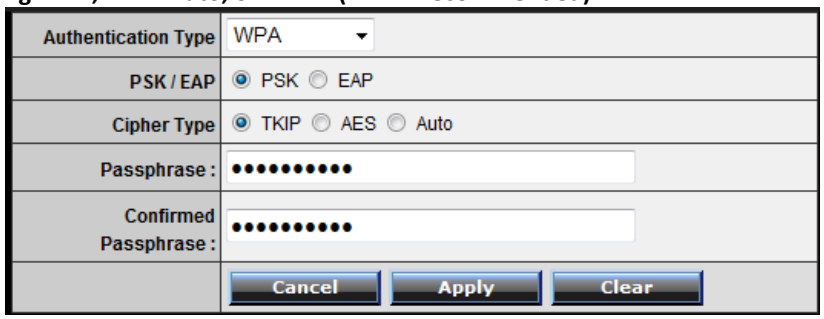
o This is where you enter the password or key needed for a computer to connect to the router wirelessly

o You can define up to 4 or 4 keys. Only one key can be active at a given time. Most users simply define one key.

o Choose a key index 1, 2, 3, or 4 and enter the key.

o When connecting to the router, the client must match both the password and the Key number. (e.g. if you have activated Key 2 with a password of 12345, then the client must select: Key 2 (entering Key 1, 3, or 4 will block the ability to connect) and enter password 12345)

Selecting WPA, WPA-Auto, or WPA2 (WPA2 recommended):



First, from the Authentication Type row, select WPA**, WPA-Auto,** or **WPA2.**

Then from the PSK/EAP row, select either PSK or EAP

- **PSK** stands for Preshared Key
- **EAP** stands for Extensive Authentication Protocol, also called Remote Authentication Dial-In User Service or RADIUS).
  Note: *EAP requires an external RADIUS server, PSK only requires you to create a passphrase.*

WEP Key Format	HEX	ASCII
Character set	0-9 & A-F, a-f only	Alphanumeric (a,b,C,?,*, /,1,2, etc.)
64-bit key length	10 characters	5 characters
128-bit key length	26 characters	13 characters

The following section outlines options when selecting PSK (Preshared Key Protocol),

o Select a Cipher Type. When selecting **WPA** security, it is recommended to use **TKIP.**

o When selecting **WPA-Auto** security, it is recommended to use **AES.**

o When selecting **WPA2** security, it is recommended to use **AES**.

© Copyright 2013 TRENDnet. All Rights Reserved.

Create your Wireless security Passphrase (password or key):

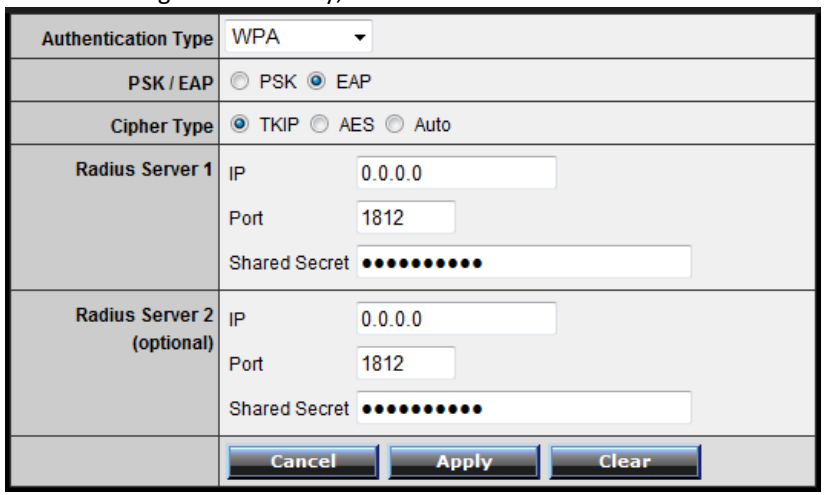
- **Passphrase:** Enter the passphrase.
- **This is the password or key that is used to connect your computer to this router wirelessly**
- **Confirmed Passphrase:** Re-enter the passphrase.
  Note: *8-63 alphanumeric characters (a,b,C,?,*, /,1,2, etc.)*

The following section outlines options when selecting EAP (Extensive Authentication Protocol),

EAP (Extensible Authentication Protocol) is also called Remote Authentication Dial-In User Service or RADIUS.

Select a Cipher Type

- o When selecting **WPA** security, it is recommended to use **TKIP.**
- o When selecting **WPA-Auto** security, it is recommended to use **AES.**
- o When selecting **WPA2** security, it is recommended to use **AES**.



- **RADIUS Server ½:** Configure the RADIUS server settings.
  Note: *RADIUS Server 2 is optional and can be configured as a backup if there are any issues with RADIUS Server 1.*
  - o **IP:** Enter the IP address of the RADIUS server. (e.g. *192.168.10.250)*
  - o **Port:** Enter the port your RADIUS server is configured to use for RADIUS authentication.

  Note: *It is recommended to use port 1812.*
  - o **Shared Secret** – Enter the shared secret used to authorize your router with your RADIUS server.

Connect wireless devices to your router

A variety of wireless network devices can connect to your wireless network such as:

- Gaming Consoles
- Internet enabled TVs
- Network media players
- Smart Phones
- Wireless Laptop computers
- Wireless IP cameras

Each device may have its own software utility for searching and connecting to available wireless networks, therefore, you must refer to the User's Manual/Guide of your wireless client device to determine how to search and connect to this router's wireless network.

See the "Appendix" on page 42 for general information on connecting to a wireless network.

© Copyright 2013 TRENDnet. All Rights Reserved.

Connect wireless devices using WPS

WPS (Wi-Fi Protected Setup) is a feature that makes it easy to connect devices to your wireless network. If your wireless devices support WPS, you can use this feature to easily add wireless devices to your network.

Note: *You will not be able to use WPS if you set the SSID Broadcast setting to Disabled.*

There are two methods the WPS feature can easily connect your wireless devices to your network.

- Push Button Configuration (PBC) method
  - o RECOMMENDED Hardware Push Button method–with an external button located physically on your router and on your client device
  - o WPS Software/Virtual Push Button - located in router management page
- PIN (Personal Identification Number) Method - located in router management page

Note: *Refer to your wireless device documentation for details on the operation of WPS.*

Recommended Hardware Push Button (PBC) Method

Note: *it is recommended that a wireless key (passphrase or password) is created before connecting clients using the PBC method. If no wireless key is defined when connecting via PBC, the router will automatically create an encryption key that is 64 characters long. This 64 character key will then have to be used if one has to connect computers to the router using the traditional connection method.*

To add a wireless device to your network, simply push the WPS button on the wireless device you are connecting(consult client device User's Guide for length of time), then push and hold the WPS button located on your router for 3 seconds and release it. A blue LED on your router WPS button will flash indicating that the WPS setup process has been activated on your router. (See "Product Hardware Features" on page 4)

For connecting additional WPS supported devices, repeat this process for each additional device.

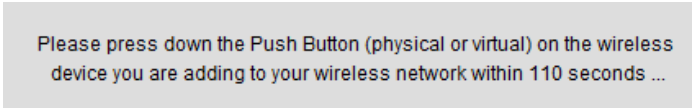
PBC (Software/Virtual Push Button)

Wireless >WiFi Protected Setup

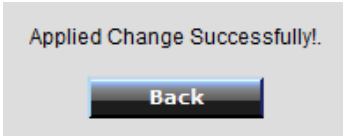
In addition to the hardware push button located physically on your router, the router management page also has push button which is a software or virtual push button you can click to activate WPS on your router.

1. Log into your router management page (see "Access your router management page" on page 24).
2. Click on **Wireless**, and click on **WPS**.
3. To add a wireless device to your network, simply the push the WPS button on the wireless device (consult wireless device's User's Guide for length of time), you are connecting, then in your router management page next to **Push Button Configuration**, click **Start PBC**.

4. You will receive a message counting down indicating the WPS process is activated on your router.


Please press down the Push Button (physical or virtual) on the wireless device you are adding to your wireless network within 110 seconds ...

5. You will receive a success message indicate that the wireless device successfully connected using WPS.



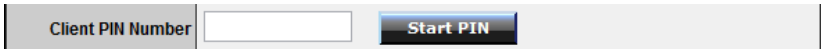
PIN (Personal Identification Number)

Wireless >WiFi Protected Setup

© Copyright 2013 TRENDnet. All Rights Reserved.

If your wireless device has WPS PIN (typically an 8-digit code printed on the wireless device product label or located in the wireless device wireless software utility), you can use this method.

1. Log into your router management page (see "Access your router management page" on page 21).
2. Click on **Wireless**, and click on **WPS**.
3. Next to **Client PIN Number**, enter the WPS PIN of the wireless device you are connecting and click **Start PIN**.



Note: *You may need to initiate the WPS PIN on your wireless device first when using this method. Refer to your wireless device documentation for details on the operation of WPS.*

Basic wireless settings

Wireless > Basic

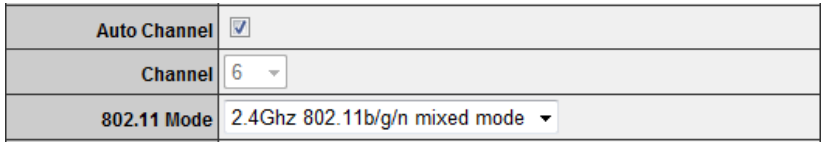
This section outlines available management options under the Basic Wireless sub tab.

1. Log into your router management page (see "Access your router management page" on page 21).
2. Click on **Wireless**, and click on **Basic**.
3. To save changes to this section, click **Apply** when finished.

- **Wireless**
  - o **Enabled** turns on the wireless networking on your router (by default it is enabled).
  - o **Disabled** turns off wireless networking on your router.

  Note: *It is recommended to leave the wireless setting to* ***Enabled*** *unless you do not plan on connecting any wireless computers or devices to your network.*

- **SSID:** This acronym stands for Service Set Identifier and is the name of your wireless network. It differentiates your wireless network from others around you. By default, the router is preconfigured with it's unique wireless network namebroadcast TRENDnet732 as the wireless network name. If you choose to change the SSID, change it to a name that you can easily remember.



- **Auto Channel:** In North America, this router can broadcast on 1 of 11 Channels (13 in Europe and other countries). Selecting Auto Channel enables the router to automatically select the best Channel for wireless communication.
- **Channel:** To manually set the channel on which the router will broadcast, uncheck **Auto Channel,** then click the drop-down list and select the desired Channel for wireless communication. The goal is to select the Channel that is least used by neighboring wireless networks.
- **802.11 Mode:** Select the appropriate mode for your network.
  - o **2.4GHz 802.11b/g/n mixed mode:** Select this mode for the best compatibility. This mode allows older 802.11b and 802.11g wireless devices to connect to the router in addition to newer 802.11n devices.
  - o **2.4GHz 802.11b/g mixed mode:** This mode only allows devices to connect to the router using older and slow 802.11b or 802.11g technology and it thereby reduces the router's maximum speed to 54Mbps (typically not recommended).
  - o **2.4GHz 802.11n only mode:** This mode only allows newer 802.11n devices to connect to your router. This mode does ensure the highest speed and security for your network, however if you have older 802.11g wireless clients, they will no longer be able to connect to this router.
  - o **2.4GHz 802.11g only mode:** This mode only allows devices to connect to the router using older and slow 802.11g technology (typically not recommended).
  - o **2.4GHz 802.11b only mode:** This mode only allows devices to connect to the router using older and slow 802.11b technology (typically not recommended).

© Copyright 2013 TRENDnet. All Rights Reserved.

Note: *Please check the specifications on your wireless devices for the highest wireless capability supported first before applying these settings. If you are unsure, it is recommended that you keep the default setting (2.4GHz 802.11b/g/n mixed mode) for the best compatibility.*

When applying the 802.11 mode setting, please keep in mind the following:

- Wireless devices that support 802.11n are backwards compatible and can connect wirelessly at 802.11g or 802.11b.
- Connecting at 802.11b or 802.11g will limit the capability of your 802.11n supported wireless devices from obtaining higher performance and data rates.
- Allowing 802.11b or 802.11g devices to connect to an 802.11n capable wireless network may degrade the wireless network performance below the higher performance and data rates of 802.11n.
- Wireless devices that only support 802.11b or 802.11g will not be able to connect to a wireless network that is set to 802.11n only mode.
- Wireless devices that only support 802.11b will not be able to connect to a wireless network that is set to 802.11g only mode.

- **Channel Width:** This setting only applies to wireless devices connecting at 802.11n. Select the appropriate channel width for your wireless network.
  - **20 MHz:** This mode operates using a single 20MHz channel for wireless devices connecting at 802.11n. This setting may provide more stability than Auto 20/40 MHz for connectivity in busy wireless environments where there are several wireless networks in the area.
  - **Auto 20/40 MHz:** This mode can automatically switch between using a single 20MHz channel or 40MHz (two 20MHz channels). When 40MHz is active, this mode is capable of providing higher performance only if the wireless devices support the 40MHz channel width. Enabling 20/40MHz typically results in substantial performance increases when connecting to an 802.11n client.
- **SSID Broadcast**
  - **Enabled** allows wireless devices to search and discover your wireless network name (also called SSID) broadcasted by your router.
  - **Disabled** turns off the ability for wireless devices to find your network. It is still possible for wireless devices to be configured to connect to your wireless network.

  Note*: Setting this option to* ***Disabled****, will disable WPS functionality****.***
- **WMM:** Wi-Fi Multimedia is a Quality of Service (QoS) feature which prioritizes audio and video data packets. This feature requires the wireless device to also support WMM. Click **Enabled (recommended)** or **Disabled** to turn this feature on or off on your router.

Steps to improve wireless connectivity

There are a number of factors that can impact the range of wireless devices. Follow these tips to help improve your wireless connectivity:

1. Keep the number of obstructions to a minimum. Each obstruction can reduce the range of a wireless device. Position the wireless devices in a manner that will minimize the amount of obstructions between them.
   a. For the widest coverage area, install your router near the center of your home, and near the ceiling, if possible.
   b. Avoid placing the router on or near metal objects (such as file cabinets and metal furniture), reflective surfaces (such as glass or mirrors), and masonry walls.
   c. Any obstruction can weaken the wireless signal (even non-metallic objects), so the fewer obstructions between the router and the wireless device, the better.
   d. Place the router in a location away from other electronics, motors, and fluorescent lighting.
   e. Many environmental variables can affect the router's performance, so if your wireless signal is weak, place the router in several locations and test the signal strength to determine the ideal position.
2. Building materials can have a large impact on your wireless signal. In an indoor environment, try to position the wireless devices so that the signal passes through less dense material such as dry wall. Dense materials like metal, solid wood, glass or even furniture may block or degrade the signal.
3. Antenna orientation can also have a large impact on your wireless signal. Use the wireless adapter's site survey tool to determine the best antenna orientation for your wireless devices.

© Copyright 2013 TRENDnet. All Rights Reserved.

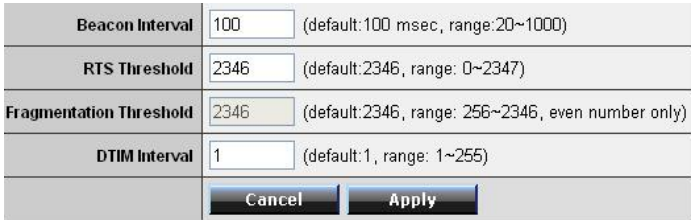
4. Interference from devices that produce RF (radio frequency) noise can also impact your signal. Position your wireless devices away from anything that generates RF noise, such as microwaves, radios and baby monitors.

If possible, upgrade wireless network interfaces (such as wireless cards in computers) from older wireless standards to 802.11n. If a wirelessly networked device uses an older standard, the performance of the entire wireless network may be slower. If you are still experiencing low or no signal consider repositioning the wireless devices or installing additional access points.

Advanced wireless settings

Wireless > Advanced

These settings are advanced options that can be configured to change advanced wireless broadcast specifications. It is recommended that these settings remain set to their default values unless you are knowledgeable about the effects of changing these values. Changing these settings incorrectly can degrade performance.



- **Beacon Interval:** A beacon is a management frame used in wireless networks that transmitted periodically to announce the presence and provide information about the router's wireless network. The interval is the amount time between each beacon transmission. Default Value:100 milliseconds (range: 20-1000)

RTS Threshold: The Request To Send (RTS) function is part of the networking protocol. A wireless device that needs to send data will send a RTS before sending the data in question. The destination wireless device will send a response called Clear to Send (CTS). The RTS Threshold defines the smallest data packet size allowed to initiate the RTS/CTS function. Default Value: 2346 (range: 0-2347)

Fragmentation Threshold: Fragmentation in wireless networks is the process of breaking down data communications into smaller data packets in order to improve data efficiency when transferring or receiving data between wireless devices. The fragmentation threshold defines the maximum size of the data packets that are broken down. Default Value: 2346 (range: 256~2346, even numbers only)

- **DTIM Interval:** A Delivery Traffic Indication Message (DTIM) is an informational message that is sent as part of a beacon by an access point (your wireless router) to a wireless client (wireless device or connecting station) in sleep mode to provide an alert that data is awaiting delivery. The DTIM Interval (also called Data Beacon Rate) is the amount of time between DTIM transmissions included in part of a beacon. Default Value: 1 (range: 1-255)

Access Control Filters

Access control basics

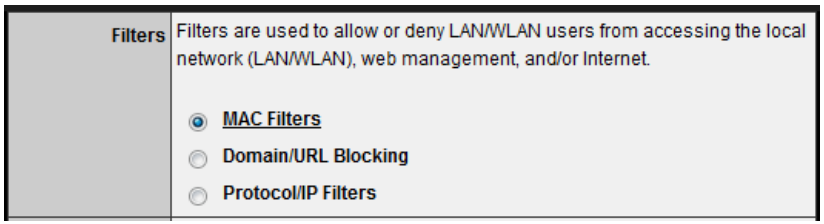
Access > Filter

MAC address filters

Access > Filter > MAC Filters

Every network device has a unique, 12-digit MAC (Media Access Control) address. Using MAC filters, you can allow or deny specific computers and other devices from using this router's wired or wireless network.

1. Log into your router management page (see "Access your router management page on page 21").
2. Click on **Access**, click on **Filter**, and click on **MAC Filters**.


Filters
Filters are used to allow or deny LAN/WLAN users from accessing the local network (LAN/WLAN), web management, and/or Internet.
MAC Filters
Domain/URL Blocking
Protocol/IP Filters

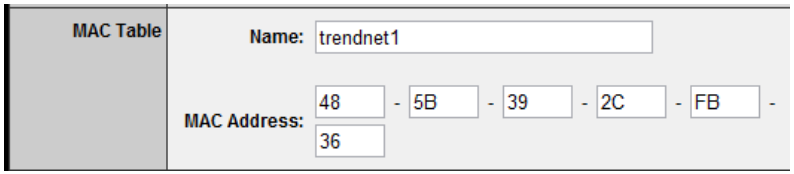
© Copyright 2013 TRENDnet. All Rights Reserved.

3. Add the MAC addresses to the MAC Table first before applying the MAC filter function.

   Note: *MAC filter can be configured to allow access to the listed MAC address and deny all others unlisted or vice versa. The recommended function is to choose to only allow access to the MAC addresses listed and deny all others unlisted because it is easier to determine the MAC addresses of devices in your network then to determine which MAC addresses you do not want to allow access.*

- **Name:** Enter a name for the MAC address entry.
- **MAC Address:** Enter the 12-digit MAC address.(e.g. *00-11-22-AA-BB-CC)*

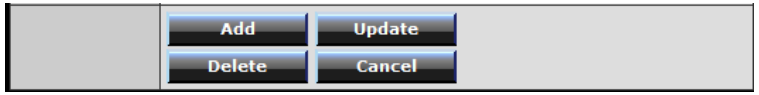
  Note: *You can check the Dynamic DHCP List for the MAC addresses of the devices on your network, see "Setup the DHCP server on your router" on page 27 or refer to your computer or device documentation to find the MAC address.*



Click **Add** to save the new MAC address entry to the MAC Table. After clicking **Add**, the MAC address entry will appear in the list below. Repeat for each device.

Name	MAC Address
trendnet1	48:5B:39:2C:FB:36

- **Add:** Saves a new MAC address entry.



To modify an existing MAC address entry, click on the entry in the MAC Table. When selected, the entry will be highlighted.

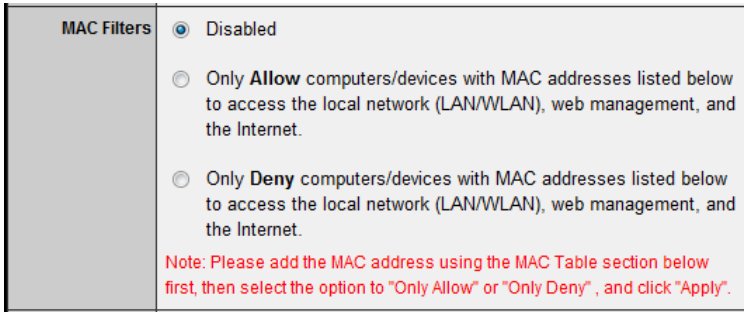
trendnet1	48:5B:39:2C:FB:36

- **Delete:** Removes an existing MAC address entry.
- **Update:** Modifies an existing MAC address entry.
- **Cancel:** Discard changes to an existing MAC address entry.

4. Review the MAC Filter options.

- **Disabled:** disables MAC address filter.
- Only **Allow** computers/devices with MAC addresses listed below to access the local network (LAN/WLAN), web management, and the Internet.
- Only **Deny** computers/devices with MAC addresses listed below to access the local network (LAN/WLAN), web management, and the Internet

  Note: *Do not configure this setting until you have added the MAC addresses to the MAC Table first. The recommended option is to only **Allow** access to the MAC addresses listed and deny all others unlisted.*


MAC Filters
Disabled
Only Allow computers/devices with MAC addresses listed below to access the local network (LAN/WLAN), web management, and the Internet.
Only Deny computers/devices with MAC addresses listed below to access the local network (LAN/WLAN), web management, and the Internet.
Note: Please add the MAC address using the MAC Table section below first, then select the option to "Only Allow" or "Only Deny" , and click "Apply".

Click **Apply** to save the changes.

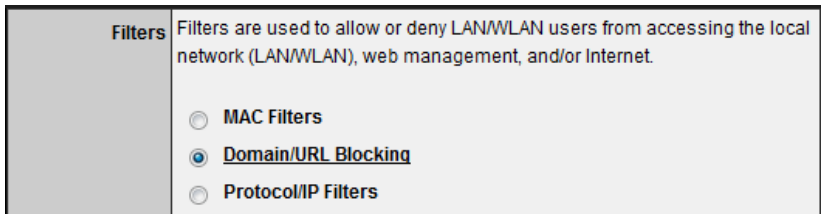
Domain/URL Filters

Access > Filter > Domain/URL Blocking

You may want to allow or block computers or devices on your network access to specific websites (e.g. *www.trendnet.com, etc.)*, also called domains or URLs (Uniform Resource Locators). You may also enter a keyword (e.g. instead of complete URL to generally allow or block computers or devices access to websites that may contain the keyword in the URL or on the web page.

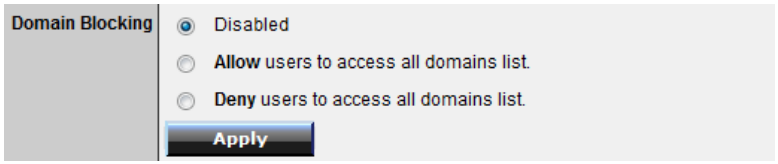
© Copyright 2013 TRENDnet. All Rights Reserved.

1. Log into your router management page (see "Access your router management page on page 21").
2. Click on **Access**, click on **Filter**, and click on **Domain/URL Blocking**.


Filters
Filters are used to allow or deny LAN/WLAN users from accessing the local network (LAN/WLAN), web management, and/or Internet.
MAC Filters
Domain/URL Blocking
Protocol/IP Filters

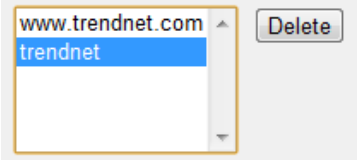
3. Review the Domain/URL blocking options.
   - **Disabled** – disables domain/URL blocking
   - **Allow** users to access all domains listed. (*Deny access to all other unlisted websites*)
   - **Deny** users to access all domains listed. (*Allow access to all other unlisted websites)*

Click **Apply** to save the changes.



4. Under Domain Blocking click on **Allow** or **Deny**. The **Domains List will then appear.** Enter the Website/URL/domain (e.g.*www.trendnet.com)* or keyword (e.g. *trendnet*) to allow or block access and click **Add** to add this to the domains list. The entry will be listed below. Repeat for each additional website or keyword added.

- **Cancel** - Discard changes to the domains list.
- **Delete** -Delete an existing website/URL/domain or keyword entry, click on the entry in the Domains List. When selected, the entry will be highlighted. Click **Delete** to remove it from the list.



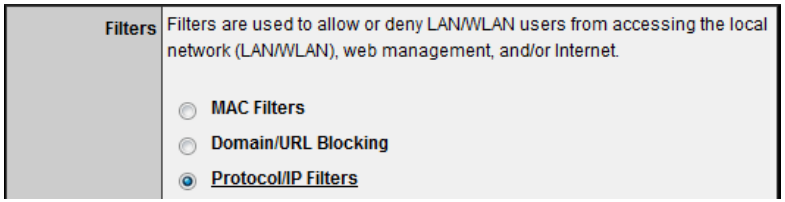
5. Go back to the Domain Blocking section and confirm you want to **Allow** or **Deny** access to the Domains List. It is generally easier to manage a list of Domains for which access is denied.
6. In Domain Blocking click on **Apply** to save the selected settings.

Protocol/IP filters

Access > Filter > Protocol/IP Filters

You may want to block computers or devices on your network access to specific ports (used or required by a specific application) to the Internet.

1. Log into your router management page (see "Access your router management page on page 21").
2. Click on **Access**, click on **Filter**, and click on **Protocol/IP Filters**.


Filters
Filters are used to allow or deny LAN/WLAN users from accessing the local network (LAN/WLAN), web management, and/or Internet.
MAC Filters
Domain/URL Blocking
Protocol/IP Filters

To simplify configuration, there is a list of commonly used pre-defined Protocol/IP Filters to modify otherwise, you can choose to manually add a new Protocol/IP Filter.

© Copyright 2013 TRENDnet. All Rights Reserved.

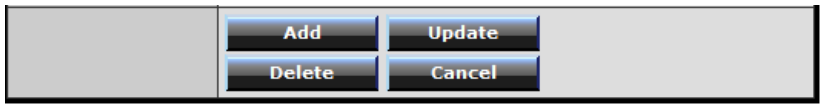
	Name	Protocol	Port Range	IP Range
☐	Filter FTP	Any	20-21	0.0.0.0-0.0.0.0
☐	Filter HTTP	Any	80-80	0.0.0.0-0.0.0.0
☐	Filter HTTPS	Any	443-443	0.0.0.0-0.0.0.0
☐	Filter DNS	Any	53-53	0.0.0.0-0.0.0.0
☐	Filter SMTP	Any	25-25	0.0.0.0-0.0.0.0
☐	Filter POP3	Any	110-110	0.0.0.0-0.0.0.0
☐	Filter Telnet	Any	23-23	0.0.0.0-0.0.0.0

3. Review the protocol/IP filter settings.

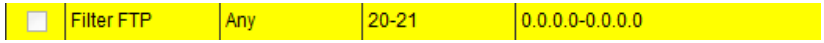
- **Enabled:** Selecting **Enabled** turns on the Protocol/IP Filter and selecting **Disabled** turns it off.
- **Name:** Enter a name for the Protocol/IP Filter.
- **Protocol:** Select the protocol type to filter. **TCP, UDP**, or you can select ***** to choose all protocol types**.**
- **Port:** Enter the port number or port range numbers to block. (e.g. *80-80* or *20-21*).
- **IP Range:** Enter the IP address or IP address range to apply the protocol/IP filter. (e.g. *192.168.10.20-192.168.10.20* or *192.168.10.20-192.168.10.30)*.

Note: *The filter will not be applied to IP addresses outside of the range specified.*

- **Add:** Saves new protocol/IP filter.



To modify an existing protocol/IP filter, click on the entry in the Protocol/IP Filters list. When selected, the entry will be highlighted.



- **Delete:** Removes an existing protocol/IP filter.
- **Update:** Modifies an existing protocol/IP filter.
- **Cancel:** Discard changes to an existing protocol/IP filter.

© Copyright 2013 TRENDnet. All Rights Reserved.

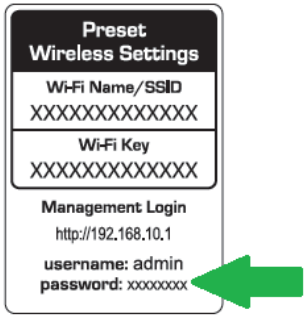
Advanced Router Setup

Access your router management page

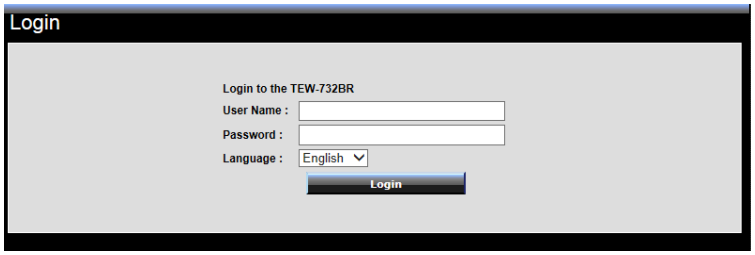
Note: *Your router management page http://192.168.10.1 is accessed through the use of your Internet web browser (e.g. Internet Explorer, Firefox, Chrome, Safari, Opera) and will be referenced frequently in this User's Guide.*

1. Open your web browser (e.g. Internet Explorer, Firefox, Safari, Chrome, or Opera) and go to http://192.168.10.1. Your router will prompt you for a user name and password.

2. Your router will prompt you for a user name and password. For added security, the router is preconfigured with a unique password. You can find the **Password** on a sticker on the side of the router and on the label on the bottom of the router.



3. Enter your **Username** and **Password**, select your preferred language, then click ***Login***.

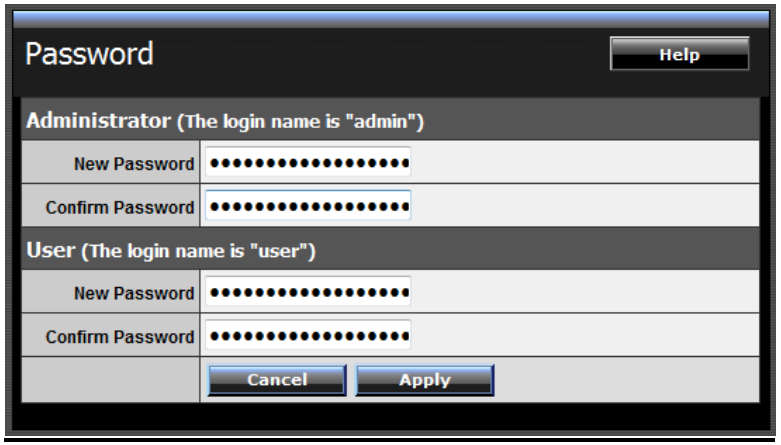


User Name: admin
Password: (xxxxxxxx)
Note: *User Name and Password are case sensitive.*

Change your router login password

Main > Password

1. Log into your router management page (see "Access your router management page" on page 21).
2. Click on **Main**, and click on **Password**.
3. Under the **Administrator** section, in the **New Password** field, enter the new password, and in the **Confirm Password** field, retype the new password again to confirm.
4. To save changes, click **Apply**.



© Copyright 2013 TRENDnet. All Rights Reserved.

Note: *If you change the router login password, you will need to access the router management page using the User Name "admin" and the new password instead of the default password "admin".*

User (Optional): The User account is an additional account used for viewing the settings on the router management page only. Accessing the router management page using the User account will restrict access to viewing only and will not allow any settings to be changed.

Default User Name: **user**

Default Password: **user**

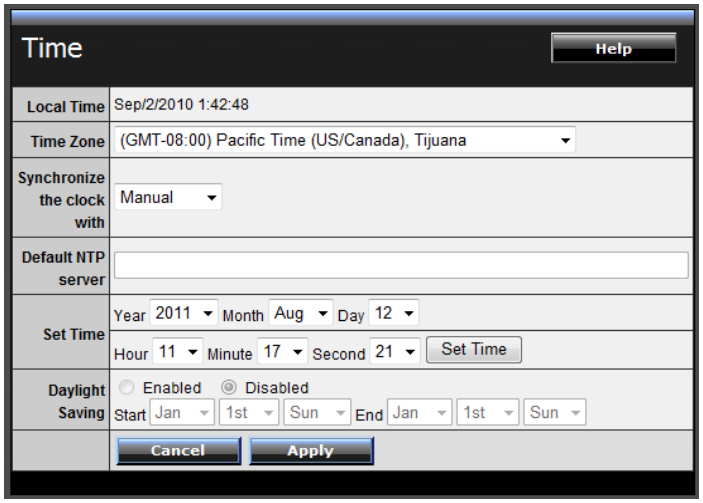
Set your router date and time

Main > Time

1. Log into your router management page (see "Access your router management page on page 21").
2. Click on **Main**, and click on **Time**.
3. Next to **Time Zone**, click the drop-down list to select your **Time Zone**.
4. Next to **Synchronize the clock with**, you can choose one of the following options:
   - **Manual:** Set your router date and time manually in the **Set Time** section. To save changes, click **Apply**.
     Note: *Time is specified in 24-hour format.*
     OR
   - **Automatic:** Set your router date and time to synchronize with an NTP (Network Time Protocol) server address (e.g. pool.ntp.org). Enter the NTP server address next to **Default NTP** server, (e.g. pool.ntp.org). Next to **Daylight Saving**, set the annual range when daylight saving is activated. To save changes, click **Apply**.

     Note*: NTP servers are used for computers and other network devices to synchronize time across an entire network.*

5. You can verify the time/date settings next to **Local Time** at the top of the page. **Local Time** displays the current date and time set on your router.

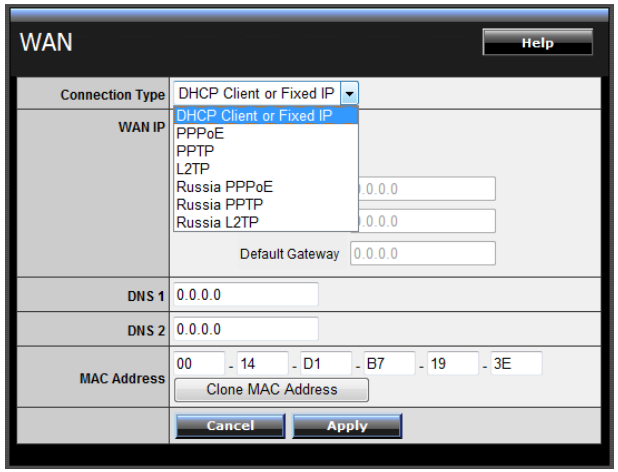


Manually configure your Internet connection

Main > WAN

1. Log into your router management page (see "Access your router management page on page 21").
2. Click on **Main**, and click on **WAN**.
3. In the **Connection Type** drop-down list, click the type of Internet connection provided by your Internet Service Provider (ISP).
4. Complete the fields required by your ISP.
5. Complete the optional settings only if required by your ISP.
6. To save changes, click **Apply**.

© Copyright 2013 TRENDnet. All Rights Reserved.



Note: *If you are unsure which Internet connection type you are using, please contact your ISP.* ***Note:*** *If your ISP requires a host name to be specified, you can specify it under Main > LAN & DHCP Server, in the* ***Host Name*** *field. To save changes, click* ***Apply*** *at bottom of the page.*

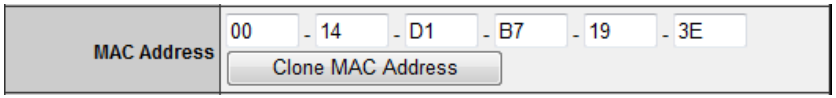
Clone a MAC address

Main > WAN

On any home network, each network device has a unique MAC (Media Access Control) address. Some ISPs register the MAC address of the device (usually a router or a computer) connected directly to the modem. If your computer MAC address is already registered with your ISP and to prevent the re-provisioning and registration process of a new MAC address with your ISP, then you can clone the address (assign the registered MAC address of your previous device to your new router). If you want to use the MAC address from the previous device (computer or old router that directly connected to the modem, you should first determine the MAC address of the device or computer and manually enter it into your router using the clone MAC address feature.

Note: *For many ISPs that provide dynamic IP addresses automatically, typically, the stored MAC address in the modem is reset each time you restart the modem. If you are installing this router for the first time, turn your modem before connecting the router to your modem. To clear your modem stored MAC address, typically the procedure is to disconnect power from the modem for approximately one minute, then reconnect the power. For more details on this procedure, refer to your modem's User Guide/Manual or contact your ISP.*

1. Log into your router management page (see "Access your router management page on page 21").
2. Click on **Main**, and click on **WAN**.
3. Under your Internet connection settings, find the **MAC Address** section shown below.



4. Click either **Clone MAC Address** to clone the MAC address of the computer you are currently using or manually enter the 12-digit MAC address of your old router.
5. To save changes, click **Apply**.

Change your router IP address

Main > LAN & DHCP Server

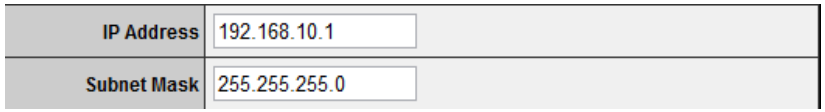
In most cases, you do not need to change your router IP address settings. Typically, the router IP address settings only needs to be changed, if you plan to use another router in your network with the same IP address settings, if you are connecting your router to an existing network that is already using the IP address settings your router is using, or if you are experiencing problems establishing VPN connections to your office network through your router.

Note: *If you are not encountering any issues or are not faced with one of the cases described above or similar, it is recommended to keep your router IP address settings as default.*

Default Router IP Address: **192.168.10.1**
Default Router Network: **192.168.10.0 / 255.255.255.0**

© Copyright 2013 TRENDnet. All Rights Reserved.

1. Log into your router management page (see "Access your router management page" on page 21).
2. Click on **Main**, and click on **LAN & DHCP Server**.
3. Enter the router IP address settings.



- **IP Address:** Enter the new router IP address. (e.g. *192.168.200.1*)
- **Subnet Mask:** Enter the new router subnet mask.(e.g. *255.255.255.0*)
  Note: *The DHCP address range will change automatically to your new router IP address settings so you do not have to change the DHCP address range manually to match your new router IP address settings.*

4. To save changes, click **Apply**.

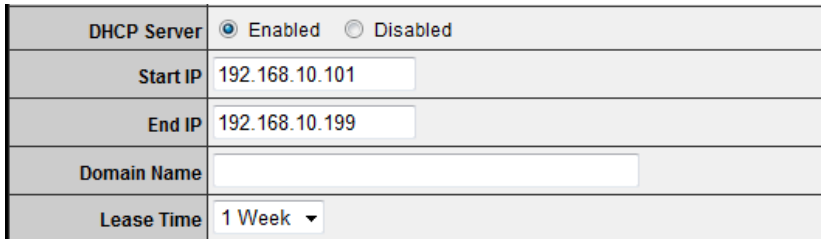
   Note: *You will need to access your router management page using your new router IP address to access the router management page. (e.g. Instead of using the default http://192.168.10.1 using your new router IP address will use the following format using your new router IP address http://(new.router.ipaddress.here) to access your router management page.*

Set up the DHCP server on your router

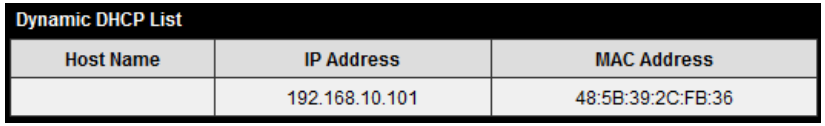
Main > LAN & DHCP Server

Your router can be used as a DHCP (Dynamic Host Configuration Protocol) server to automatically assign an IP address to each computer or device on your network. The DHCP server is enabled by default on your router. If you already have a DHCP server on your network, or if you do not want to use your router as a DHCP server, you can disable this setting. It is recommended to leave this setting enabled.

1. Log into your router management page (see "Access your router management page" on page 21).
2. Click on **Main**, and click on **LAN & DHCP Server**.
3. Review the DHCP Server settings.
   - **DHCP Server:** Enable or Disable the DHCP server.
   - **Start IP:** Changes the starting address for the DHCP server range. (e.g. *192.168.10.20)*
   - **End IP:** Changes the last address for the DHCP server range. (e.g. *192.168.10.30)*
     Note: *The Start IP and End IP specify the range of IP addresses to automatically assign to computers or devices on your network.*
   - **Domain Name (Optional):** Specifies a domain name to assign to computers or devices. (e.g. *trendnet.com*)
   - **Lease Time:** Click the drop-down list to select the lease time.
     Note: *The DHCP lease time is the amount of time a computer or device can keep an IP address assigned by the DHCP server. When the lease time expires, the computer or device will renew the IP address lease with the DHCP server, otherwise, if there is no attempt to renew the lease, the DHCP server will reallocate the IP address to be assigned to another computer or device.*
4. To save changes, click **Apply**.



Dynamic DHCP List – You can view the list of active lease entries for computers or devices that have been assigned IP addresses automatically from the DHCP server on your router.



© Copyright 2013 TRENDnet. All Rights Reserved.

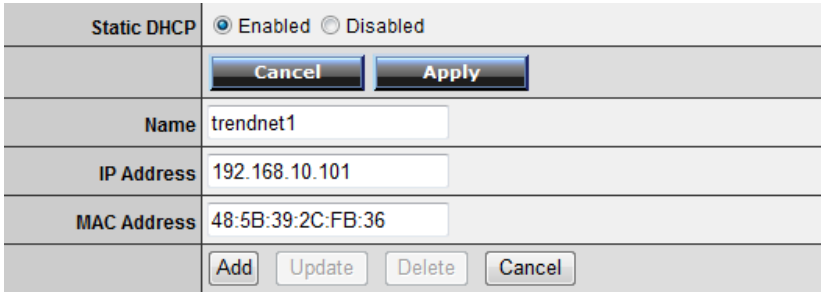
Set up DHCP reservation

Main > LAN & DHCP Server

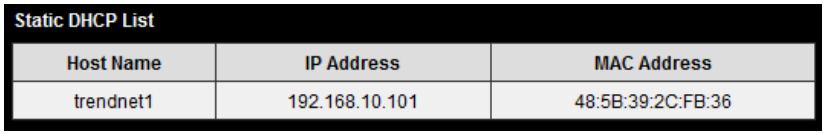
DHCP (Dynamic Host Configuration Protocol) reservation (also called Static DHCP) allows your router to assign a fixed IP address from the DHCP server IP address range to a specific device on your network. Assigning a fixed IP address can allow you to easily keep track of the IP addresses used on your network by your computers or devices for future reference or configuration such as virtual server (also called port forwarding, see "Virtual Server" on page 28) or special applications (also called port triggering, see "Special Applications" on page 30).

1. Log into your router management page (see "Access your router management page" on page 21).
2. Click on **Main**, and click on **LAN & DHCP Server**.
3. Review the DHCP reservation settings.

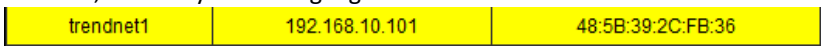
- **Static DHCP:** Enable or Disable the DHCP reservation feature.
- **Name:** Enter a name for the reservation.
- **IP Address:** Enter the IP address to assign to the reservation. (e.g. 192.168.10.101)
  Note: *You cannot assign IP addresses outside of the DHCP range. The IP address is required to be within the DHCP IP address range (Start IP & End IP).*
- **MAC Address:** Enter the MAC (Media Access Control) address of the computer or network device to assign to the reservation. (e.g. *00:11:22:AA:BB:CC)*
- **Add:** Saves the reservation.



Static DHCP List – You can view the list of reservations for computers or devices that have been created in this list.



To modify an existing reservation, click on the entry in the Static DHCP list. When selected, the entry will be highlighted.



- **Update:** Saves changes to an existing reservation.
- **Delete:** Removes an existing reservation.
- **Cancel:** Discards changes to existing reservation.

Enable/disable UPnP on your router

Management > Remote Management

UPnP (Universal Plug and Play) allows devices connected to a network to discover each other and automatically open the connections or services for specific applications (e.g. instant messenger, online gaming applications, etc.) UPnP is enabled on your router by default to allow specific applications required by your computers or devices to allow connections through your router as they are needed.

1. Log into your router management page (see "Access your router management page" on page 21).
2. Click on **Management**, and click on **Remote Management**.
3. Next to **UPnP**, click **Enabled** or **Disabled** to turn the feature on or off on your router.

   Note: *It is recommended to leave this setting enabled, otherwise, you may encounter issues with applications that utilize UPnP in order allow the required communication between your computers or devices and the Internet.*
4. To save changes, click **Apply**.

© Copyright 2013 TRENDnet. All Rights Reserved.

Allow/deny VPN connections through your router

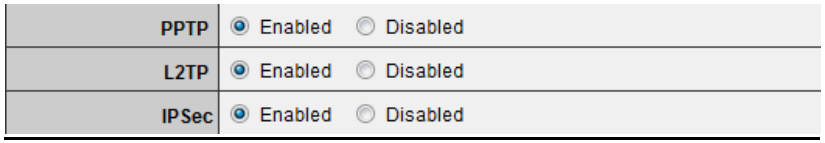
Management > Remote Management

A Virtual Private Network (VPN) is a network that uses a public network, such as the Internet, to provide secure communications between a remote computer or network and another network. Some offices often provide VPN access to their networks to enable employees to work from their remote office/home office, or while traveling.

If your office or place of work has allowed and authorized access for you to access their network through VPN, the default VPN settings in your router have been configured to pass through the most common types of VPN protocols, which typically do not require any additional configuration changes.

1. Log into your router management page (see "Access your router management page" on page 21).
2. Click on **Management**, and click on **Remote Management**.
3. Next to **PPTP, L2TP, or IPsec** (depending the VPN protocol your corporation requires) click **Enabled** or **Disabled** to turn the VPN pass through feature on or off on your router.

   Note: *It is recommended to leave these settings enabled.*
4. To save changes, click **Apply**.



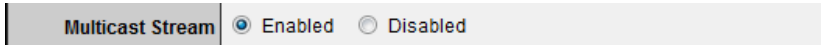
Allow/deny multicast streaming

Management > Remote Management

In some cases, applications require multicast communication (also called IP multicast which is the delivery of information to a specific group of computers or devices in a single transmission) typically used in media streaming applications. Multicast streaming is enabled by default on your router to allow applications that require multicast communication through your router which typically does not require additional configuration changes.

1. Log into your router management page (see "Access your router management page" on page 21).
2. Click on **Management**, and click on **Remote Management**.
3. Next to **Multicast Stream**, click **Enabled** or **Disabled** to turn the feature on or off on your router.

   Note: *It is recommended to leave this setting enabled.*
4. To save changes, click **Apply**.



Identify your network on the Internet

Main > Dynamic DNS

Since most ISPs constantly change your home IP address, providing access to devices on your home or small office Local Area Network (such as IP Cameras) from the Internet requires setting up a Dynamic DNS service and entering the parameters into this management area. Dynamic DNS services allow your router to confirm its location to the given Dynamic DNS service, thereby providing the Dynamic DNS service with the ability to provide a virtual fixed IP address for your network. This means that even though your ISP is always changing your IP address, the Dynamic DNS service will be able to identify your network using a fixed address—one that can be used to view home IP Camera and other devices on your local area network.

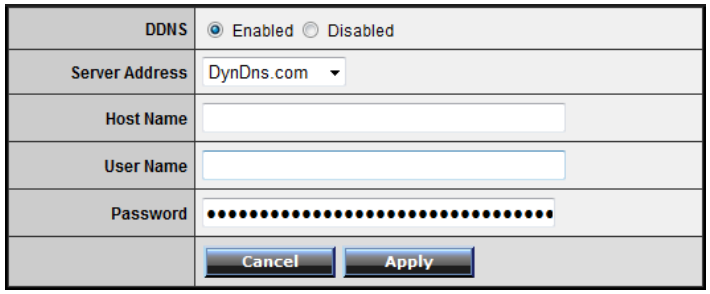
Note: *First, you will need to sign up for one of the DDNS service providers listed in the* ***Server Address*** *drop-down list.*

1. Sign up for one of the DDNS available service providers list under **Server Address**. (e.g. *dyndns.com, no-ip.com*, etc.)
2. Log into your router management page (see "Access your router management page" on page 21).
3. Click on **Main** and click on **Dynamic DNS**.
4. Next to DDNS, click **Enabled.**
5. In the **Server Address** drop-down list, select the provider you selected, and enter your information in the fields.

© Copyright 2013 TRENDnet. All Rights Reserved.

- Host Name: Personal URL provided to you by your Dynamic DNS service provider (e.g. www.trendnet.dyndns.biz)
- **User Name:** The user name needed to log in to your Dynamic DNS service account
- **Password:** This is the password to gain access to Dynamic DNS service (NOT your router or wireless network password) for which you have signed up to.

6. To save changes, click **Apply**.



Allow remote access to your router management page

Management > Remote Management

You may want to make changes to your router from a remote location such at your office or another location while away from your home.

1. Log into your router management page (see "Access your router management page" on page 21).
2. Click on **Management**, and click on **Remote Management**.
3. Under the **HTTP** section, click **Enabled**.
   - **Port:** It is recommended to leave this setting as 8080.
     Note: *If you have configured port 8080 for another configuration section such as virtual server or special application, please change the port to use. (Recommended port range 1024-65534)*
   - **Remote IP Range:** It is recommended to leave this setting as *, to allow remote access from anywhere on the Internet.
     Note*: You can enter a specific range of Internet IP addresses that are allowed to access your router management page, all others will be denied.*

4. To save changes, click **Apply**.

Open a device on your network to the Internet

This router can provide access to devices on your local area network to the Internet using the Virtual Server, Special Application, method (DMZ NOT recommended).

DMZ

Access > DMZ

You may want to expose a specific computer or device on your network to the Internet to allow anyone to access it. Your router includes the DMZ (Demilitarized Zone) feature that makes all the ports and services available on the WAN/Internet side of the router and forwards them to a single IP address (computer or network device) on your network. The DMZ feature is an easy way of allowing access from the Internet however, it is a very **insecure** technology and will open local area network to greater threats from Internet attacks.

It is strongly recommended to use **Virtual Server** (also called port forwarding, see "Virtual Server" on page 28) to allow access to your computers or network devices from the Internet.

1. Make the computer or network device (for which you are establishing a DMZ link) has a static IP address (or you can use the DHCP reservation feature to ensure the device has a fixed IP address) (see "Set up DHCP reservation" on page 25).

   A. Signing up for a Dynamic DNS service (outlined in the DDNS section) will provide identification of the router's network from the Internet.
2. Log into your router management page (see "Access your router management page" on page 21).
3. Click on **Access**, and click on **DMZ**.

© Copyright 2013 TRENDnet. All Rights Reserved.

4. Next to **DMZ Enable**, click **Enabled**.
5. Next to **DMZ Host IP**, enter the IP address you assigned to the computer or network device to expose to the Internet.
6. To save changes, click **Apply**.

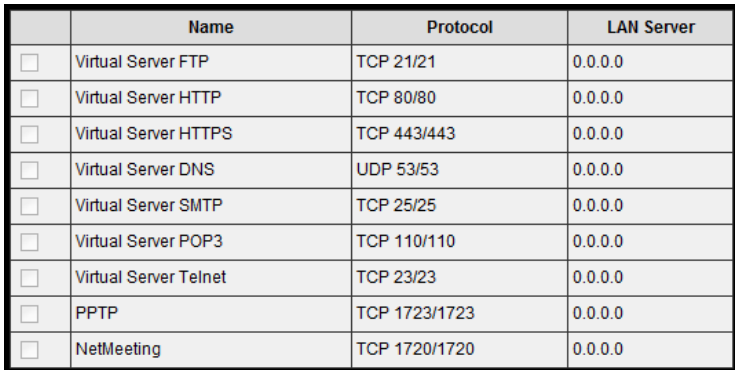
Virtual Server

Access > Virtual Server

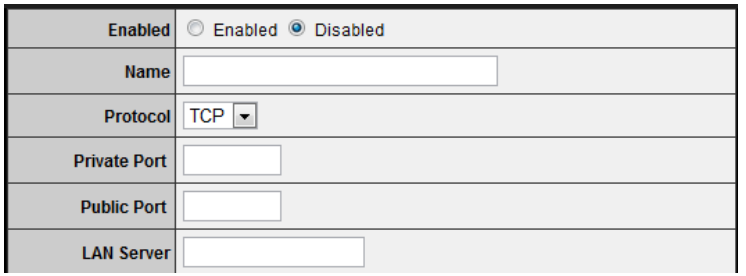
Virtual Server (also called port forwarding) allows you to define specific ports (used or required by a specific application) and forward them to a single IP address (a computer or device) on your network. Using this feature is more secure compared to using DMZ (see DMZ on page 27) in which DMZ forwards all ports instead of only specific ports used by an application. An example would be forwarding a port to an IP camera (TRENDnet IP cameras default to HTTP TCP port 80 for remote access web requests) on your network to be able to view it over the Internet.

Since most ISPs constantly change your home IP address, to be able to access the Virtual Server port(s) from the Internet it is recommended to setup Dynamic DNS service (See DynDNS section).

1. Log into your router management page (see "Access your router management page" on page 21).
2. Click on **Access**, and click on **Virtual Server**.



To simplify configuration, there is a list of commonly used pre-defined virtual server entries to modify, otherwise, you can choose to manually add a new virtual server.



3. Review the virtual server settings.

- **Enabled:** Selecting **Enabled** turns on the virtual server and selecting **Disabled** turns off the virtual server.
- **Name:** Enter a name for the virtual server.
- **Protocol:** Select the protocol required for your device. **TCP**, **UDP**, or you can select **Both** to choose both TCP & UDP (recommended).

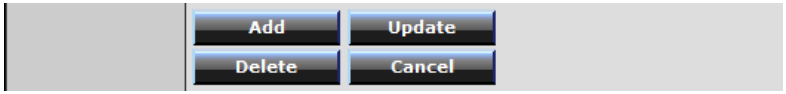
  Note: *Please refer to the device documentation to determine which ports and protocols are required.*
- **Private Port:** Enter the port number required by your device. Refer to the connecting device's documentation for reference to the network port(s) required.
- **Public Port:** Enter the port number used to access the device from the Internet.

© Copyright 2013 TRENDnet. All Rights Reserved.

Note: *The* ***Public Port*** *can be assigned a different port number than the* ***Private Port*** *(also known as port redirection), however it is recommended to use the same port number for both settings. Please refer to the device documentation to determine which ports and protocols are required.*

- **LAN Server:** Enter the IP address of the device to forward the port (e.g. *192.168.10.101)*.

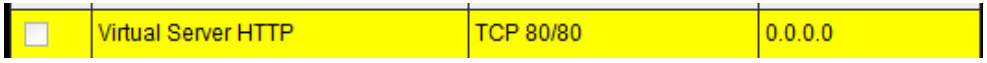
  Note: You should assign a static IP address to the device or use DHCP reservation to ensure the IP address of the device does not change.
- **Add:** Saves a new virtual server entry.
- **Delete:** Removes an existing virtual server.
- **Update:** Modifies an existing virtual server.
- **Cancel:** Discard changes to an existing virtual server.



Example: To forward TCP port 80 to your IP camera

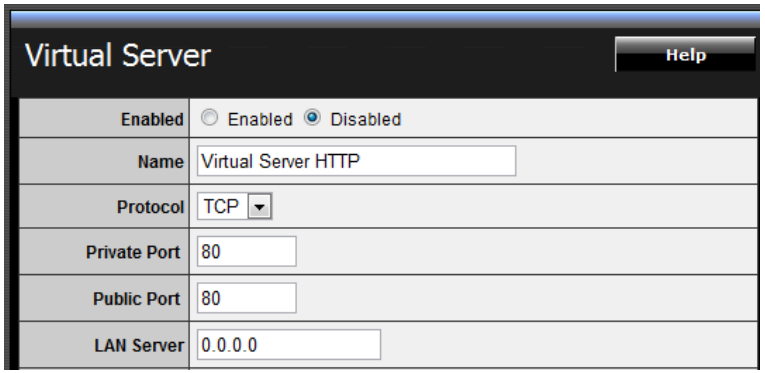
1. Setup DynDNS service (See DynDNS section).
2. Access TRENDnet IP Camera management page and forward Port 80 (see product documentation)
3. Make sure to configure your network/IP camera to use a static IP address or you can use the DHCP reservation feature (see "Set up DHCP reservation" on page 25).

   Note: *You may need to reference your camera documentation on configuring a static IP address.*
4. Log into your router management page (see "Access your router management page" on page 21).
5. Click on **Access**, and click on **Virtual Server**.
6. In the list below, click the pre-defined virtual server entry named **Virtual Server HTTP**.



Note: *The selected item will be highlighted in yellow when selected.*

7. The fields will be populated with the selected pre-defined virtual server entry.



8. Click **Enabled** to turn on this virtual server.
9. Next to **Name**, you can enter another name for the virtual server, otherwise, leave the default name.
10. Next to **Protocol**, make sure **TCP** is selected in the drop-down list.
11. The **Private Port** and **Public Port**, make sure port number **80** is configured for both settings.
12. Next to **LAN Server**, enter the IP address assigned to the camera. (e.g. *192.168.10.101*)
13. To save the changes, click **Update.**

Special Applications

Access > Special AP

Special applications (also called port triggering) is typically used for online gaming applications or communication applications that require a range of ports or several ports to be dynamically opened on request to a device on your network. The router will wait for a request on a specific port or range of ports (or trigger port/port range) from a device on your network and once a request is detected by your router, the router will forward a single port or multiple ports (or incoming port/port range) to the device on your network. This feature is not typically used as most devices and routers currently

© Copyright 2013 TRENDnet. All Rights Reserved.

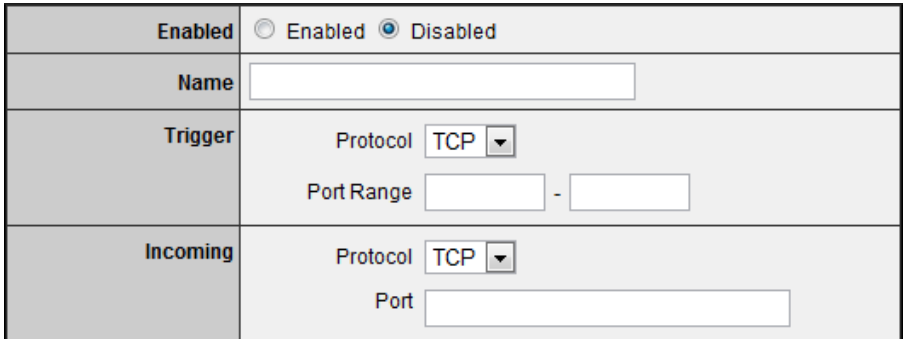
use UPnP (Universal Plug and Play) to automatically configure your router to allow access for applications. See "Enable/disable UPnP on your router" on page 25.

Note: *Please refer to the device documentation to determine if your device supports UPnP first, before configuring this feature.*

1. Log into your router management page (see "Access your router management page" on page 21).
2. Click on **Access**, and click on **Special AP**.

	Name	Trigger Port Range	Incoming Port
☐	Battle.net	Any 6112-6112	Any 6112
☐	Dialpad	Any 7175-7175	Any 51200-51201,51210
☐	ICU II	Any 2019-2019	Any 2000-2038,2025-2051,2069,2085,3010-3030
☐	PC-to-Phone	Any 12053-12053	Any 12120,12122,24150-24220
☐	Quick Time 4	Any 554-554	Any 6970-6999

To simplify configuration, there is a list of commonly used pre-defined special application entries to modify, otherwise, you can choose to manually add a new special application.



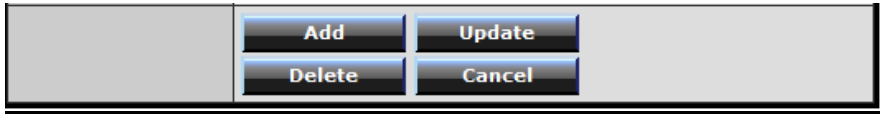
3. Review the special application settings.

- **Enabled:** Selecting **Enabled** turns on the special application and selecting **Disabled** turns it off.
- **Name:** Enter a name for the special application.
- **Trigger:** Port or port range requested by the device.
  - o **Protocol:** Select the protocol requested by the device. **TCP, UDP**, or you can select **Both** to choose both TCP and **UDP.**
  - o **Port Range:** Enter the ports or port range requested by the device. (e.g. *554-554 or 6112-6112).*

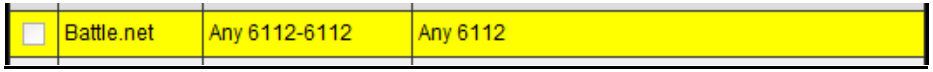
  Note: *Please refer to the device documentation to determine which ports and protocols are required.*
- **Incoming:** Port(s) forwarded to the device.
  - o **Protocol:** Select the protocol to be forwarded to the device. **TCP, UDP**, or you can select **Both** to choose both TCP and **UDP.**
  - o **Port Range:** Enter the ports or port range to be forwarded to the device.

    (e.g. *2000-2038,2069,2081,2200-2210).*

  Note: *Please refer to the device documentation to determine which ports and protocols are required.*
- **Add:** Saves a new special application.



To modify an existing application, click on the entry in the special applications list. When selected, the entry will be highlighted.



- **Delete:** Removes an existing special application.
- **Update:** Modifies an existing special application.
- **Cancel:** Discard changes to an existing special application.

© Copyright 2013 TRENDnet. All Rights Reserved.

Add static routes to your router

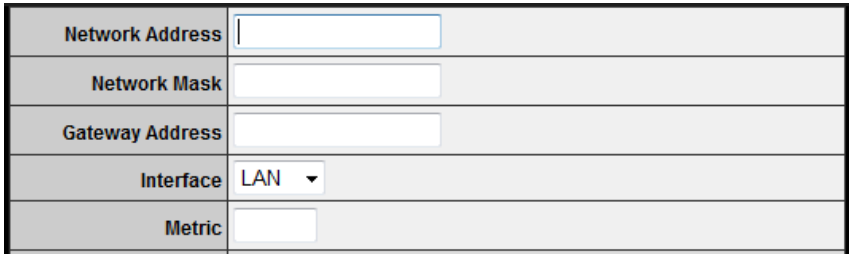
Routing > Static

You may want set up your router to route computers or devices on your network to other local networks through other routers. Generally, different networks can be determined by the IP addressing assigned to those networks. Generally speaking and for the case of an example, your network may have 192.168.10.x IP addressing and another network may have 192.168.20.x IP addressing and because the IP addressing of these two networks are different, they are separate networks. In order to communicate between the two separate networks, static routing needs to be configured. Below is an example diagram where routing is needed for devices and computers on your network to access the other network.

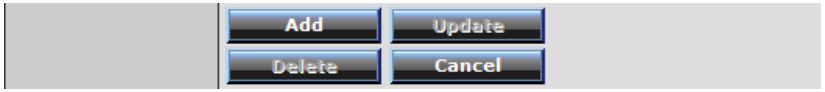
Note: *Configuring this feature assumes that you have some general networking knowledge.*

1. Log into your router management page (see "Access your router management page" on page 21).
2. Click on **Routing**, and click on **Static**.
3. Review the static route settings.

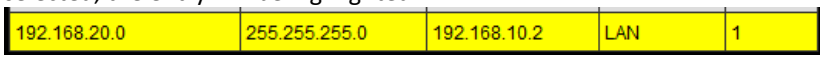
- **Network Address:** Enter the IP network address of the destination network for the route. (e.g. *192.168.20.0*)
- **Network Mask:** Enter the subnet mask of the destination network for the route.(e.g. *255.255.255.0*)
- **Gateway Address:** Enter the gateway to the destination network for the route.(e.g. 192.168.10.2)
- **Interface:** Click the drop-down list and select the Interface on your router where the route is active. (e.g. *LAN*)
- **Metric:** Enter the metric or priority of the route. The metric range is *1-16*, the lowest number *1* being the highest priority. (e.g. *1*)



- **Add:** Saves the static route.



To modify an existing reservation, click on the entry in the static route list. When selected, the entry will be highlighted.



- **Update:** Saves changes to an existing static route.
- **Delete:** Removes an existing static route.
- **Cancel:** Discards changes to existing static route.

Router Maintenance & Monitoring

Reset your router to factory defaults

Tools > Settings

You may want to reset your router to factory defaults if you are encountering difficulties with your router and have attempted all other troubleshooting. Before you reset your router to defaults, if possible, you should backup your router configuration first, see "Backup and restore your router configuration settings" on page 32.

There are two methods that can be used to reset your router to factory defaults.

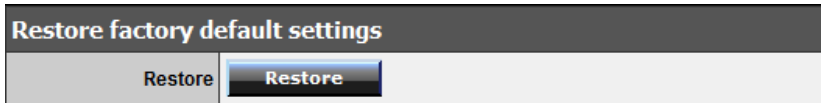
© Copyright 2013 TRENDnet. All Rights Reserved.

- **Reset Button:** Located on the rear panel of your router, see "Product Hardware Features" on page 4. Use this method if you are encountering difficulties with accessing your router management page.

  OR

- **Router Management Page**

1. Log into your router management page (see "Access your router management page" on page 21).
2. Click on **Tools** and click on **Settings**.
3. Under **Restore factory default settings**, click **Restore**. When prompted to confirm this action, click **OK**.



Router Default Settings

Administrator User Name	admin
Administrator Password	admin
Router IP Address	192.168.10.1
Router Subnet Mask	255.255.255.0
DHCP Server IP Range	192.168.10.101-192.168.199
Wireless	Enabled
SSID (wireless network name)	TRENDnet732
Wireless Security	Wireless security is based on the device serial number. ***Note:*** *Please see device label for the default wireless security key*
802.11 Mode	2.4GHz 802.11b/g/n mixed mode
Channel	Auto Channel

Backup and restore your router configuration settings

Tools > Settings

You may have added many customized settings to your router and in the case that you need to reset your router to default, all your customized settings would be lost and would require you to manually reconfigure all of your router settings instead of simply restoring from a backed up router configuration file.

To backup your router configuration:

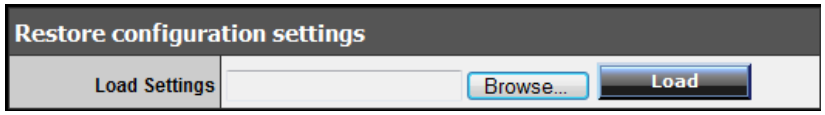
1. Log into your router management page (see "Access your router management page" on page 21).
2. Click on **Tools** and click on **Settings**.
3. Under **Save Configuration Settings** and next to **Save Settings**, click **Save**.

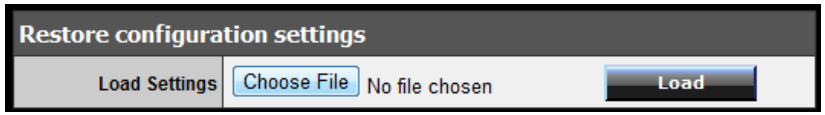
4. Depending on your web browser settings, you may be prompted to save a file (specify the location) or the file may be downloaded automatically to the web browser settings default download folder. (Default Filename: *cfg.bin)*

To restore your router configuration:

1. Log into your router management page (see "Access your router management page" on page 21).
2. Click on **Tools** and click on **Settings**.
3. Under **Restore Configuration Settings**, next to **Load Settings**, depending on your web browser, click on **Browse** or **Choose File**.

© Copyright 2013 TRENDnet. All Rights Reserved.





4. A separate file navigation window should open.Select the router configuration file to restore and click **Load**.

   (Default Filename: *cfg.bin*). If prompted, click **Yes** or **OK**.

5. Wait for the router to restore settings.

Upgrade your router firmware

Tools > Firmware

TRENDnet may periodically release firmware upgrades that may add features or fix problems associated with your TRENDnet router model and version. To check if there is a firmware upgrade available for your device, please check your TRENDnet model and version using the link. http://www.trendnet.com/downloads/

In addition, it is also important to verify if the latest firmware version is newer than the one your router is currently running. To identify the firmware that is currently loaded on your router, log in to the router, click on the Status tab and then on the Device Information sub-tab. The firmware used by the router is listed at the top of this page. If there is a newer version available, also review the release notes to check if there were any new features you may want or if any problems were fixed that you may have been experiencing.

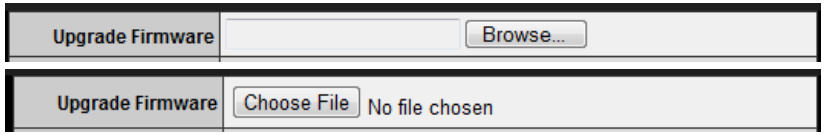
1. If a firmware upgrade is available, download the firmware to your computer.
2. Unzip the file to a folder on your computer.

Please note the following:

- Do not interrupt the firmware upgrade process. Do not turn off the device or press the Reset button during the upgrade.
- If you are upgrade the firmware using a laptop computer, ensure that the laptop is connected to a power source or ensure that the battery is fully charged.
- Disable sleep mode on your computer as this may interrupt the firmware upgrade process.
- Do not upgrade the firmware using a wireless connection, only using a wired network connection.
- Any interruptions during the firmware upgrade process may permanently damage your router.

1. Log into your router management page (see "Access your router management page on page 21").
2. Click on **Status** and click on **Device Information** to check your router's current firmware version at the top of the page.

3. Click on **Tools** and click on **Firmware**.
4. Depending on your web browser, next to **Upgrade Firmware**, click **Browse** or **Choose File**.



5. Navigate to the folder on your computer where the unzipped firmware file (*.bin*) is located and select it.
6. Click **Upgrade**. If prompted, click **Yes** or **OK**.

© Copyright 2013 TRENDnet. All Rights Reserved.

Restart your router

Tools > Restart

You may want to restart your router if you are encountering difficulties with your router and have attempted all other troubleshooting.

There are two methods that can be used to restart your router.

- **Turn the router off** for 10 seconds using the router On/Off switch located on the rear panel of your router, see "Product Hardware Features" on page 4.

  Note: *Use this method if you are encountering difficulties with accessing your router management page. This is also known as a hard reboot or power cycle.*

  OR

- **Router Management Page:** This is also known as a soft reboot or restart.

1. Log into your router management page (see "Access your router management page" on page 21).
2. Click on **Tools** and click on **Restart**. If prompted, click **Yes** or **OK**.

Check connectivity using the router management page

Tools > Ping Test

For troubleshooting purposes, you may want to check your router connectivity using the ping (also known as a network connectivity test) test tool on your router management page.

1. Log into your router management page (see "Access your router management page" on page 21).
2. Click on **Tools** and click on **Ping Test**.
3. Enter in the IP address (e.g. *192.168.10.101*) or host name (e.g. www.*trendnet.com*) to test.
4. Click **Ping**.

5. You will receive a *success* or *fail* result message of the address you entered providing a basic indicating of the router's connectivity to the Internet or devices that are connected to your network. Click **Back** to bring you back to the **Ping Test** page.

Check the router system information

Status > Device Information

You may want to check the system information of your router such as WAN (Internet) connectivity, wireless and wired network settings, router MAC address, and firmware version.

1. Log into your router management page (see "Access your router management page" on page 21).
2. Click on **Status** and click on **Device Information**.
3. Review the device information.
   - **Firmware Version:** The current firmware version your router is running.
   - **Router Up Time:** The duration your router has been running continuously without a restart/power cycle (hard or soft reboot) or reset.

WAN (Internet) Information

© Copyright 2013 TRENDnet. All Rights Reserved.

- **MAC Address:** The current MAC address used by your router's WAN port or interface configuration.
- **Connection:** Displays the current WAN (Internet) connection status. When using DHCP Client (or Dynamic IP address) Internet connection type, you will provide the option to Release and Renew your IP address settings. Renew Release

  Note: *Other Internet connection types such as PPPoE will provide the option to Connect and Disconnect.* Connect Disconnect
- **IP Address:** The current IP address assigned to your router WAN port or interface configuration.
- **Subnet Mask:** The current subnet mask assigned to your router WAN port or interface configuration.
- **Default Gateway:** The current gateway assigned to your router WAN port or interface configuration.
- **DNS (Domain Name System):** The current DNS address(es) assigned to your router port or interface configuration.

WAN	
MAC Address	
Connection	
IP Address	
Subnet Mask	
Default Gateway	
DNS	

Wireless Information

- **MAC Address:** The current MAC address of your router's wireless or interface configuration.
- **Connection:** Displays the status if your wireless functionality on your router is enabled or disabled.
- **SSID:** Displays the current wireless network name assigned to your router.
- **Channel:** Displays the current wireless channel your router is operating.
- **Authentication:** Displays the current wireless security configured on your router.

Wireless	
MAC Address	
Connection	
SSID	
Channel	
Authentication	

Wired LAN Information

- **MAC Address:** The current MAC address of your router's wired LAN or interface configuration.
- **IP Address:** Displays your router's current IP address.
- **Subnet Mask:** Displays your router's current subnet mask.
- **DHCP Server:** Display your router's DHCP server status, enabled or disabled, and provides a link to the DHCP client listing. DHCP Table

LAN	
MAC Address	
IP Address	
Subnet Mask	
DHCP Server	

View your router log

Status > Log

Your router log can be used to obtain activity information on the functionality of your router or for troubleshooting purposes.

1. Log into your router management page (see "Access your router management page on page 21").
2. Click on **Status** and click on **Log**.
3. Review the device log information.

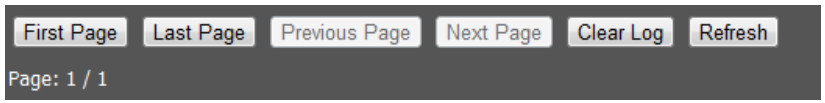
© Copyright 2013 TRENDnet. All Rights Reserved.

- **Time:** Displays the time of the log entry. If the time is inaccurate, make sure to set the router date and time correctly. (See "Set your router date and time" on page 22)
- **Type:** Displays a notification regarding the type of log.
- **Message:** Displays the log message.

Time	Type	Message
Sep 1 01:38:57	user.warn	kernel: wlan0: A STA is expired - 00:14:D1:90:5E:A7
Sep 1 01:38:53	user.warn	kernel: wlan0: A wireless client is associated - 7C:ED:8D:2E:9F:B3
Sep 1 01:38:53	user.warn	kernel: wlan0: A wireless client is associated - 7C:ED:8D:2E:9F:B3

Router Log Navigation

- **First Page:** Displays the first page of the log.
- **Last Page:** Displays the last page of the log.
- **Previous Page:** Display the log page previous to the current. The **Page: 1/1** will display the current page.
- **Next Page:** Displays the log page next to the current.
- **Clear Log:**- Clears all logging
- **Refresh:** The **Page: 1/1** will display the current page.



Configure your router log

Status > Log Setting

You may want send your router log to your e-mail address or to an external log server (also known as Syslog server) so you can check it periodically while away from home. You may also want to only see specific categories of logging.

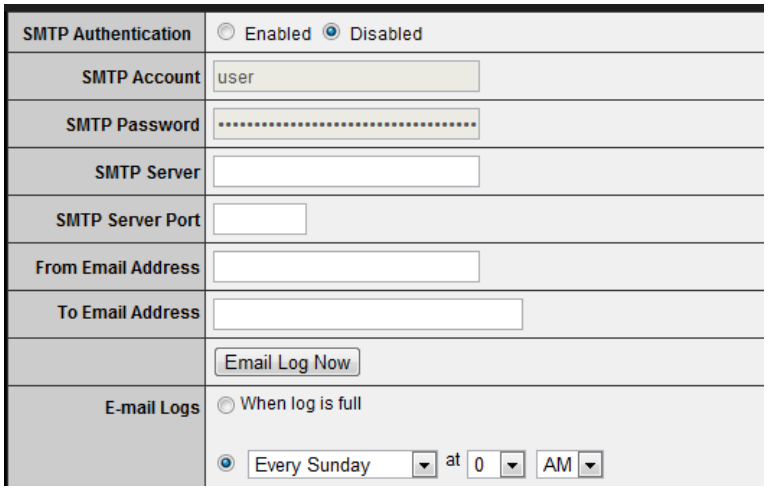
Send router logs to your e-mail address

1. Log into your router management page (see "Access your router management page" on page 21).
2. Click on **Status** and click on **Log Setting**.
3. Review the e-mail log settings.
   - **SMTP Authentication:** Set this option to **Enabled** if your e-mail service requires authentication. If not, leave this setting to **Disabled**.

     Note: *If you are unsure of this setting check with your e-mail service provider if authentication is required.*
   - **SMTP Account:** Enter your account user name for your e-mail service.
   - **SMTP Password:** Enter your password for your e-mail service.
   - **SMTP Server:** Enter the IP address (e.g. *10.10.10.10*) or domain name (e.g. *mail.trendnet.com*) of your e-mail server.
   - **SMTP Server Port:** Enter the port used by your e-mail service. (e.g. *Default SMTP Server Port: 25*)
   - **From Email Address:** Enter a sender e-mail address. (e.g. *router@trendnet.com*)

     Note: *This does not need to be real e-mail address, only used for identification purposes when checking your e-mail.*
   - **To Email Address:** Enter your e-mail address.
   - **Email Log Now:** Click this option to send an e-mail with the current router log using your email settings.
   - **Email Logs:** Select when you want the router log to be e-mailed.
     - **When log is full:** The router log will be e-mailed to your e-mail address when router internal log is full.
     - Click the drop-down list and configure to e-mail logs according to a set schedule. Once on a specific day of the week or once every day.

© Copyright 2013 TRENDnet. All Rights Reserved.



4. To save changes, click **Apply**.

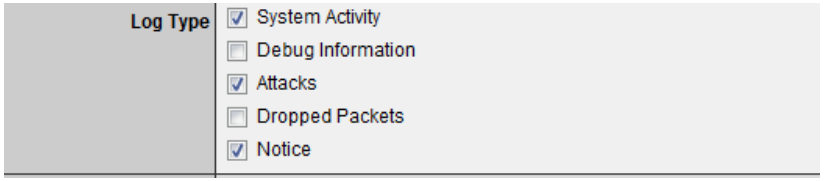
Send router logs to an external log server

1. Log into your router management page (see "Access your router management page" on page 21).
2. Click on **Status** and click on **Log Setting**.
3. Next to **Syslog Server**, enter the IP address of the external log server to send router logging.

4. To save changes, click **Apply**.

Set the types or categories to include in logging

1. Log into your router management page (see "Access your router management page" on page 21).
2. Click on **Status** and click on **Log Setting**.
3. Next to **Log Type**, check the types or categories to include in logging.



4. To save changes, click **Apply**.

View your router packet statistics

Status > Statistics

You may want to check your router packet statistics for informational purposes only.

1. Log into your router management page (see "Access your router management page" on page 21).
2. Click on **Status** and click on **Statistic**.
3. The table displays the amount of packets sent and received on your router's wired LAN, wireless, and WAN (Internet).

Utilization (packets)		LAN	Wireless	WAN
Send	Peak	60175	8661	18701
Receive	Peak	49091	272459	13773

© Copyright 2013 TRENDnet. All Rights Reserved.

View wireless devices connected to your router

Status > Wireless

You may want to check the wireless devices connected to your router.

1. Log into your router management page (see "Access your router management page" on page 21).
2. Click on **Status** and click on **Wireless**.
3. The table displays the amount time each wireless device has been connected and the MAC address of each wireless device.

Connected Time	MAC Address
01:06:31	7c:ed:8d:2e:9f:b3

© Copyright 2013 TRENDnet. All Rights Reserved.

Router Management Page Structure

Main

- LAN & DHCP Server
  - Static DHCP Reservation
- WAN
  - Clone MAC Address
- Password
- Time
- Dynamic DNS

Wireless

- Basic
- Security
- Advanced
- Wi-Fi Protected Setup

Status

- Device Information
- Log
- Log Setting
  - Email Log
  - Syslog
  - Log Type
- Statistic
- Wireless

Routing

- Static
- Routing Table

Access

- Filter
  - MAC Filters
  - Domain/URL Blocking
  - Protocol/IP Filters
- Virtual Server
- Special AP
- DMZ

Management

- Remote Management
  - Remote Management
  - Allow Ping to WAN port
  - UPnP

Tools

- Restart
- Settings
  - Save Configuration Settings
  - Restore Configuration Settings
  - Reset to Factory Default
- Firmware
  - Upgrade Firmware
- Ping Test

Wizard

- Setup Wizard

© Copyright 2012 TRENDnet. All Rights Reserved.

Technical Specifications

Hardware	
Standards	IEEE 802.3 (10BASE-T), IEEE 802.3u (100BASE-TX), IEEE 802.11b, IEEE 802.11g, Based on IEEE 802.11n technology, IEEE 802.3az
WAN	1 x 10/100Mbps Auto-MDIX WAN port (Internet)
LAN	4 x 10/100Mbps Auto-MDIX LAN ports
WPS Button	Enables Wi-Fi Protected Setup (WPS) function (Hold for 3 seconds)
Power Switch	On/Off power switch
Connection Type	Dynamic IP, Static (fixed) IP, PPPoE, PPTP, L2TP
Supported Web Browsers	Internet Explorer 6.0 or above, Firefox 2.0 or above, Chrome, Opera, Safari
Internet Access Control	MAC Address Filter, Domain/URL Filter, Protocol/IP Filter, Virtual Server, DMZ host, UPnP, PPTP/L2TP/IPsec VPN pass through
Management / Monitoring	Local/remote configuration, upgrade firmware, Backup/Restore configuration via Web browser, Internal System Log, Syslog, E-Mail Logging, Ping Test Tool, Dynamic DNS
Routing	Static
LED Indicators	Power, Internet
Power	Input: 100~240V AC, 50~60Hz Output: 5V DC, 1A
Power Consumption	3 Watts (max)
Dimensions (L x W x H)	150 x 60 x 112 mm (6 x 2.3 x 4.4 in)
Weight	198 g (7 oz)
Temperature	Operating: 0° ~ 40°C (32° ~ 104°F) Storage: -10°C ~ 70°C (-14° ~ 158°F)
Humidity	Max. 95% (non-condensing)
Certifications	CE, FCC
Wireless	
Frequency	2.412 ~ 2.472 GHz ISM band
Antenna	2 x 2 dBi internal antenna
Modulation	DBPSK/DQPSK/CCK/OFDM (BPSK/QPSK/16-QAM/64-QAM)
Media Access Protocol	CSMA/CA with ACK
Data Rate	802.11b: up to 11 Mbps 802.11g: up to 54 Mbps 802.11n: up to 300 Mbps
Output Power	802.11b: 18.3 dBm (typical) @ 11 Mbps 802.11g: 21.1 dBm (typical) @ 54 Mbps 802.11n: 22.9 dBm (typical) @ 300Mbps HT 40MHz
Receiving Sensitivity	802.11b: -85 dBm (typical) @ 11 Mbps 802.11g: -68 dBm (typical) @ 54 Mbps 802.11n: -64 dBm (typical) @ 300 Mbps
Encryption	64/128-bit WEP (HEX/ASCII), WPA /WPA2-PSK, WPA/WPA2-RADIUS
Channels	1-11 (FCC), 1-13 (ETSI)

*Maximum wireless signal rates are referenced from IEEE 802.11 theoretical specifications. Actual data throughput and coverage will vary depending on interference, network traffic, building materials and other conditions.

© Copyright 2013 TRENDnet. All Rights Reserved.

Troubleshooting

Q: I typed http://192.168.10.1 in my Internet Browser Address Bar, but an error message says "The page cannot be displayed." How can I access the router management page?
Answer:
1. Check your hardware settings again. See "Router Installation" on page 7.
2. Make sure the LAN and WLAN lights are lit.
3. Make sure your network adapter TCP/IP settings are set to *Obtain an IP address automatically* or *DHCP* (see the steps below).
4. Make sure your computer is connected to one of the router's LAN ports
5. Press on the factory reset button for 5 seconds, the release.

Windows 7

a. Go into the **Control Panel**, click **Network and Sharing Center**.

b. Click **Change Adapter Settings**, right-click the **Local Area Connection** icon.

c. Then click **Properties** and click **Internet Protocol Version 4 (TCP/IPv4)**.

d. Then click **Obtain an IP address automatically** and click **OK**.

Windows Vista

a. Go into the Control Panel, click Network and Internet.

b. Click Manage Network Connections, right-click the Local Area Connection icon and click Properties.

c. Click Internet Protocol Version (TCP/IPv4) and then click Properties.

d. Then click Obtain an IP address automatically and click OK.

Windows XP/2000

a. Go into the Control Panel, double-click the Network Connections icon

b. Right-click the Local Area Connection icon and the click Properties.

c. Click Internet Protocol (TCP/IP) and click Properties.

d. Then click Obtain an IP address automatically and click OK.

Note: *If you are experiencing difficulties, please contact your computer or operating system manufacturer for assistance.*

Q: I am not sure what type of Internet Account Type I have for my Cable/DSL connection. How do I find out?
Answer:
Contact your Internet Service Provider (ISP) for the correct information.

Q: The Wizard does not appear when I access the router. What should I do?
Answer:
1. Click on Wizard on the left hand side.
2. Near the top of the browser, "Pop-up blocked" message may appear. Right click on the message and select Always Allow Pop-ups from This Site.
3. Disable your browser's pop up blocker.

Q: I went through the Wizard, but I cannot get onto the Internet. What should I do?
Answer:
1. Verify that you can get onto the Internet with a direct connection into your modem (meaning plug your computer directly to the modem and verify that your single computer (without the help of the router) can access the Internet).
2. Power cycle your modem and router. Unplug the power to the modem and router. Wait 30 seconds, and then reconnect the power to the modem. Wait for the modem to fully boot up, and then reconnect the power to the router.
3. Contact your ISP and verify all the information that you have in regards to your Internet connection settings is correct.

Q: I cannot connect wirelessly to the router. What should I do?
Answer:
1. Double check that the WLAN light on the router is lit.
2. Power cycle the router. Unplug the power to the router. Wait 15 seconds, then plug the power back in to the router.
3. Contact the manufacturer of your wireless network adapter and make sure the wireless network adapter is configured with the proper SSID. The preset SSID is TRENDnet(*model_number)*.
4. To verify whether or not wireless is enabled, login to the router management page, click on *Wireless*.
5. Please see "Steps to improve wireless connectivity" on page 16 if you continue to have wireless connectivity problems.

© Copyright 2013 TRENDnet. All Rights Reserved.

Appendix

How to find your IP address?

Note: *Please note that although the following procedures provided to follow for your operating system on configuring your network settings can be used as general guidelines, however, it is strongly recommended that you consult your computer or operating system manufacturer directly for assistance on the proper procedure for configuring network settings.*

Command Prompt Method

Windows 2000/XP/Vista/7

1. On your keyboard, press **Windows Logo+R** keys simultaneously to bring up the Run dialog box.
2. In the dialog box, type ***cmd*** to bring up the command prompt.
3. In the command prompt, type ***ipconfig /all*** to display your IP address settings.

MAC OS X

1. Navigate to your **Applications** folder and open **Utilities**.
2. Double-click on **Terminal** to launch the command prompt.
3. In the command prompt, type ***ipconfig getifaddr <en0 or en1>*** to display the wired or wireless IP address settings.

Note: en0 *is typically the wired Ethernet and* ***en1*** *is typically the wireless Airport interface.*

Graphical Method

MAC OS 10.6/10.5

1. From the Apple menu, select **System Preferences**.
2. In System Preferences, from the **View** menu, select **Network**.
3. In the Network preference window, click a network port (e.g., Ethernet, AirPort, modem). If you are connected, you'll see your IP address settings under "Status:"

MAC OS 10.4

1. From the Apple menu, select **Location**, and then **Network Preferences**.
2. In the Network Preference window, next to "Show:", select **Network Status**. You'll see your network status and your IP address settings displayed.

Note: *If you are experiencing difficulties, please contact your computer or operating system manufacturer for assistance.*

How to configure your network settings to obtain an IP address automatically or use DHCP?

Note: *Please note that although the following procedures provided to follow for your operating system on configuring your network settings can be used as general guidelines, however, it is strongly recommended that you consult your computer or operating system manufacturer directly for assistance on the proper procedure for configuring network settings.*

Windows 7

a. Go into the **Control Panel**, click **Network and Sharing Center**.

b. Click **Change Adapter Settings**, right-click the **Local Area Connection** icon.

c. Then click **Properties** and click **Internet Protocol Version 4 (TCP/IPv4)**.

d. Then click **Obtain an IP address automatically** and click **OK**.

Windows Vista

a. Go into the **Control Panel**, click **Network and Internet**.
b. Click **Manage Network Connections,** right-click the **Local Area Connection** icon and click **Properties**.
c. Click **Internet Protocol Version (TCP/IPv4)** and then click **Properties**.
d. Then click **Obtain an IP address automatically** and click **OK**.

Windows XP/2000

a. Go into the **Control Panel**, double-click the **Network Connections** icon
b. Right-click the **Local Area Connection** icon and the click **Properties**.
c. Click **Internet Protocol (TCP/IP)** and click **Properties**.
d. Then click **Obtain an IP address automatically** and click **OK**.

MAC OS 10.4/10.5/10.6

a. From the **Apple**, drop-down list, select **System Preferences**.
b. Click the **Network** icon.
c. From the **Location** drop-down list, select **Automatic**.
d. Select and view your Ethernet connection.
In MAC OS 10.4, from the **Show** drop-down list, select **Built-in Ethernet** and select the **TCP/IP** tab.
In MAC OS 10.5/10.6, in the left column, select **Ethernet**.
e. Configure TCP/IP to use DHCP.

© Copyright 2013 TRENDnet. All Rights Reserved.

In MAC 10.4, from the **Configure IPv4**, drop-down list, select **Using DHCP** and click the **Apply Now** button.
In MAC 10.5, from the **Configure** drop-down list, select **Using DHCP** and click the **Apply** button.
In MAC 10.6, from the **Configure** drop-down list, select **Using DHCP** and click the **Apply** button.

f. Restart your computer.

Note: *If you are experiencing difficulties, please contact your computer or operating system manufacturer for assistance.*

How to find your MAC address?

In Windows 2000/XP/Vista/7,

Your computer MAC addresses are also displayed in this window, however, you can type ***getmac –v*** to display the MAC addresses only.

In MAC OS 10.4,

1. **Apple Menu > System Preferences > Network**
2. From the **Show** menu, select **Built-in Ethernet**.
3. On the **Ethernet** tab, the **Ethernet ID** is your MAC Address.

In MAC OS 10.5/10.6,

1. **Apple Menu > System Preferences > Network**
2. Select **Ethernet** from the list on the left.
3. Click the **Advanced** button.
3. On the **Ethernet** tab, the **Ethernet ID** is your MAC Address.

How to connect to a wireless network using the built-in Windows utility?

Note: *Please note that although the following procedures provided to follow for your operating system on configuring your network settings can be used as general guidelines, however, it is strongly recommended that you consult your computer or operating system manufacturer directly for assistance on the proper procedure for connecting to a wireless network using the built-in utility.*

Windows 7

1. Open Connect to a Network by clicking the network icon (or) in the notification area.
2. In the list of available wireless networks, click the wireless network you would like to connect to, then click **Connect.**
4. You may be prompted to enter a security key in order to connect to the network.
5. Enter in the security key corresponding to the wireless network, and click **OK**.

Windows Vista

1. Open Connect to a Network by clicking the **Start Button**. and then click **Connect To.**
2. In the **Show** list, click **Wireless**.
3. In the list of available wireless networks, click the wireless network you would like to connect to, then click **Connect.**
4. You may be prompted to enter a security key in order to connect to the network.
5. Enter in the security key corresponding to the wireless network, and click **OK**.

Windows XP

1. Right-click the network icon in the notification area, then click **View Available Wireless Networks**.
2. In **Connect to a Network**, under **Available Networks**, click the wireless network you would like to connect to.
3. You may be prompted to enter a security key in order to connect to the network.
4. Enter in the security key corresponding to the wireless network, and click **Connect**.

© Copyright 2013 TRENDnet. All Rights Reserved.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

-Reorient or relocate the receiving antenna.

-Increase the separation between the equipment and receiver.

-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

-Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

RoHS

This product is RoHS compliant.

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

EN60950-1: 2010

Safety of Information Technology Equipment

EN 50385: 2002

Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public

EN 300 328 V1.7.1 (2006-10)

Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive

EN 301 489-1 V1.8.1 (2008-04)

Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

EN 301 489-17 V2.1.1 (2009-05)

Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

© Copyright 2013 TRENDnet. All Rights Reserved.

cs Česky [Czech]	TRENDnet tímto prohlašuje, že tento TEW-732BR je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
da Dansk [Danish]	Undertegnede TRENDnet erklærer herved, at følgende udstyr TEW-732BR overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
de Deutsch [German]	Hiermit erklärt TRENDnet, dass sich das Gerät TEW-732BR in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
et Eesti [Estonian]	Käesolevaga kinnitab TRENDnet seadme TEW-732BR vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
en English	Hereby, TRENDnet, declares that this TEW-732BR is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
es Español [Spanish]	Por medio de la presente TRENDnet declara que el TEW-732BR cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ TRENDnet ΔΗΛΩΝΕΙ ΟΤΙ TEW-732BR ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
fr Français [French]	Par la présente TRENDnet déclare que l'appareil TEW-732BR est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
it Italiano [Italian]	Con la presente TRENDnet dichiara che questo TEW-732BR è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
lv Latviski [Latvian]	Ar šo TRENDnet deklarē, ka TEW-732BR atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
lt Lietuvių [Lithuanian]	Šiuo TRENDnet deklaruoja, kad šis TEW-732BR atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
nl Nederlands [Dutch]	Hierbij verklaart TRENDnet dat het toestel TEW-732BR in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
mt Malti [Maltese]	Hawnhekk, TRENDnet, jiddikjara li dan TEW-732BR jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
hu Magyar [Hungarian]	Alulírott, TRENDnet nyilatkozom, hogy a TEW-732BR megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
pl Polski [Polish]	Niniejszym TRENDnet oświadcza, że TEW-732BR jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
pt Português [Portuguese]	TRENDnet declara que este TEW-732BR está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
sl Slovensko [Slovenian]	TRENDnet izjavlja, da je ta TEW-732BR v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
sk Slovensky [Slovak]	TRENDnet týmto vyhlasuje, že TEW-732BR spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
fi Suomi [Finnish]	TRENDnet vakuuttaa täten että TEW-732BR tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
sv Svenska [Swedish]	Härmed intygar TRENDnet att denna TEW-732BR står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

© Copyright 2013 TRENDnet. All Rights Reserved.

Limited Warranty

TRENDnet warrants its products against defects in material and workmanship, under normal use and service, for the following lengths of time from the date of purchase.

TEW-732BR – 3 Years Warranty

AC/DC Power Adapter, Cooling Fan, and Power Supply carry 1 year warranty.

If a product does not operate as warranted during the applicable warranty period, TRENDnet shall reserve the right, at its expense, to repair or replace the defective product or part and deliver an equivalent product or part to the customer. The repair/replacement unit's warranty continues from the original date of purchase. All products that are replaced become the property of TRENDnet. Replacement products may be new or reconditioned. TRENDnet does not issue refunds or credit. Please contact the point-of-purchase for their return policies.

TRENDnet shall not be responsible for any software, firmware, information, or memory data of customer contained in, stored on, or integrated with any products returned to TRENDnet pursuant to any warranty.

There are no user serviceable parts inside the product. Do not remove or attempt to service the product by any unauthorized service center. This warranty is voided if (i) the product has been modified or repaired by any unauthorized service center, (ii) the product was subject to accident, abuse, or improper use (iii) the product was subject to conditions more severe than those specified in the manual.

Warranty service may be obtained by contacting TRENDnet within the applicable warranty period and providing a copy of the dated proof of the purchase. Upon proper submission of required documentation a Return Material Authorization (RMA) number will be issued. An RMA number is required in order to initiate warranty service support for all TRENDnet products. Products that are sent to TRENDnet for RMA service must have the RMA number marked on the outside of return packages and sent to TRENDnet prepaid, insured and packaged appropriately for safe shipment. Customers shipping from outside of the USA and Canada are responsible for return shipping fees. Customers shipping from outside of the USA are responsible for custom charges, including but not limited to, duty, tax, and other fees.

WARRANTIES EXCLUSIVE: IF THE TRENDNET PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT TRENDNET'S OPTION, REPAIR OR REPLACE. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. TRENDNET NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF TRENDNET'S PRODUCTS.

TRENDNET SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW TRENDNET ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATE, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT TRENDNET'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Governing Law: This Limited Warranty shall be governed by the laws of the state of California.

Some TRENDnet products include software code written by third party developers. These codes are subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL").

Go to http://www.trendnet.com/gpl or http://www.trendnet.com Download section and look for the desired TRENDnet product to access to the GPL Code or LGPL Code. These codes are distributed WITHOUT WARRANTY and are subject to the copyrights of the developers. TRENDnet does not provide technical support for these codes. Please go to http://www.gnu.org/licenses/gpl.txt or http://www.gnu.org/licenses/lgpl.txt for specific terms of each license.

PWP05202009v2 2013/9/10

© Copyright 2013 TRENDnet. All Rights Reserved.

TRENDnet®

Product Warranty Registration

Please take a moment to register your product online.
Go to TRENDnet's website at http://www.trendnet.com/register

TRENDnet
20675 Manhattan Place
Torrance, CA 90501. USA

Copyright ©2013. All Rights Reserved. TRENDnet.